TILBURG UNIVERSITY

Watermerken als juridisch bewijsmiddel

Gellaerts, S.L.

Document version:
Publisher's PDF, also known as Version of record

Publication date:
2015

Link to publication

Citation for published version (APA):
Gellaerts, S. L. (2015). Watermerken als juridisch bewijsmiddel: Een onderzoek naar de effectiviteit van digitale watermerken als juridisch bewijsmiddel S.l.: [s.n.]

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

? Users may download and print one copy of any publication from the public portal for the purpose of private study or research
? You may not further distribute the material or use it for any profit-making activity or commercial gain
? You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright, please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. sep. 2016

Watermerken als juridisch bewijsmiddel

Watermerken als juridisch bewijsmiddel

Een onderzoek naar de effectiviteit van digitale watermerken als juridisch bewijsmiddel

Proefschrift
ter verkrijging van de graad
van doctor aan Tilburg University
op gezag van de rector magnificus, prof. dr. E.H.L. Aarts,
in het openbaar te verdedigen ten overstaan van een
door het college voor promoties aangewezen commissie
in de aula van de Universiteit op
maandag 28 september 2015 om 10.15 uur door
Sander Gellaerts

Promotor: Prof. mr. drs. C. Stuurman
Copromotor: Mr. ir. M.H.M. Schellekens

Leden: Prof. dr. mr. P.J.A. De Hert
Prof. dr. A. Dooms
Prof. mr. I. Giesen
Prof. mr. A.A. Quaedvlieg
Prof. dr. mr. T.F.E. Tjong Tjin Tai

ISBN/EAN: 978-94-91602-38-2

De paginanummers in deze digitale versie wijken niet af van die in het gedrukte exemplaar.

© 2015 S. Gellaerts | CC BY-SA 4.0
Hoewel aan de totstandkoming van dit werk de uiterste zorg is besteed, aanvaarden noch de auteur noch anderen enige aansprakelijkheid voor eventuele fouten en onvolkomenheden of voor de gevolgen daarvan.

Aanbevolen citeerwijze: S.L. Gellaerts, *Watermerken als juridisch bewijsmiddel. Een onderzoek naar de effectiviteit van digitale watermerken als juridisch bewijsmiddel*, 2015.

Inhoudsopgave

1 Inleiding 1

1.1 Digitale watermerken als juridisch bewijsmiddel 1

1.2 Probleemstelling en nadere afbakening 2

1.3 Doel en methode van onderzoek 5

1.3.1 Onderzoeksmethoden: juridisch-normatief en rechtsvergelijkend onderzoek 5

1.3.2 Selectie van een rechtsstelsel 8

1.3.3 Rechtsvergelijking 9

1.4 Verantwoording 10

1.4.1 Onderzoekskader: IM-PACT-project 10

1.4.2 Verslag van de onderzoeksbevindingen 12

1.4.3 Taalkeuze: lingua franca of onderzoeksratio 15

1.5 Plan van behandeling 15

2 Watermerken als technisch bewijsmiddel 19

2.1 Inleiding 19

2.2 Introductie digitale watermerken als techniek 20

2.2.1 Korte geschiedenis van watermerken 20

2.2.2 Classificatie van watermerken 25

2.2.3 Digitaal watermerken als techniek 27

2.2.4 Toepassingen van watermerktechnieken 30

2.2.5 Authenticatie van de licentienemer 33

2.3 Het proces van watermerken; van aanbrengen tot interpretatie 36

2.3.1 Aanbrengen 36

2.3.2 Verspreiden 39

2.3.3 Detecteren 39

2.3.4 Interpretatie 44

2.3.5 Tussenconclusie: risico’s ten aanzien van de betrouwbaarheid 44

2.4 Eigenschappen van watermerksystemen en -technieken 46
2.4.1 Detectie 47
2.4.2 Embedden 49
2.4.3 Waarneembaarheid 51
2.4.4 Capaciteit 52
2.4.5 Robuustheid 53
2.4.6 Beveiliging 54
2.4.7 Kosten 56
2.4.8 Tussenconclusie: over keuzes en betrouwbaarheid 57
2.5 Meest aannemelijke aanvallen 58
2.5.1 Life-cycle benadering van Carver e.a. 59
2.5.2 Voorkomen van detectie of vervals-benadering van Cox e.a. 61
2.5.3 De type-indeling van Kutter e.a. 63
2.6 Samenvatting en conclusie 64

3 Watermerken en handhaving van het auteursrecht 69

3.1 Inleiding 69
3.2 De rol van het watermerk bij handhaving van auteursrecht 70
3.2.1 Watermerken: DRM met een vriendelijk gezicht 71
3.2.2 Watermerken in het licht van de drijfveren van up- en downloaders 74
3.3 De plaats van watermerken in het handhavingsbeleid 78
3.3.1 Handhavingsbeleid van overheidswege 79
3.3.1.1 Europese Unie 79
3.3.1.2 Nederland 83
3.3.1.3 België 87
3.3.2 Particulier handhavingsbeleid 90
3.3.2.1 Nederland 91
3.3.2.2 België 93
3.3.3 Tussenconclusie 94

3.4 Watermerken en het probandum 96
3.4.1 Inbreuk op het auteursrecht als onrechtmatige daad 97
3.4.1.1 Nederland 97
3.4.1.2 België 100
3.4.1.3 Tussenconclusie 103
3.4.2 Inbreuk op het auteursrecht als strafbaar feit 104
3.4.2.1 Nederland 104
3.4.2.2 België 107
3.4.2.3 Tussenconclusie 110
3.5 Auteursrechtelijke bescherming van watermerken 111
3.5.1 Omzeilen van technische voorzieningen 112
3.5.1.1 Nederland 112
3.5.1.2 België 115
3.5.2 Bescherming van elektronische gebruiksinformatie 116
3.5.2.1 Nederland 116
3.5.2.2 België 118
3.5.3 Tussenconclusie 118
3.6 Samenvatting en conclusie 119

4 Watermerken als bewijs in een juridische procedure 123

4.1 Inleiding 123
4.2 Beslissen over feiten naar Nederlands civiel recht 124
4.2.1 Bewijsrisicoverdeling 125
4.2.1.1 Stellen en betwisten 126
4.2.1.2 Bewijslastverdeling 134
4.2.1.3 Bewijsaanbod, bewijsopdracht en bewijslevering 140
4.2.2 Aannemelijke verweren 141
4.2.3 Beslissen over feiten: het bewijsoordeel 144
4.2.3.1 Beslissen over watermerken 145
4.2.3.2 Debat: de bewijswaarderingsmaatstaf van De Bock & watermerken. 151
4.2.3.3 De deskundige als betrouwbare informant 160
4.2.4 Tussenconclusie 163

4.3 Beslissen over feiten naar Belgisch civiel recht 164
4.3.1 Bewijsrisicoverdeling 167
4.3.1.1 Aanvoeringsrechten en -plichten 168
4.3.1.2 Bewijslastverdeling 171
4.3.2 Aannemelijke verweren 174
4.3.3 Beslissen over feiten: het bewijsoordeel 175
4.3.3.1 Beslissen over watermerken 176
4.3.3.2 De deskundigen als betrouwbare informant 178
4.3.4 Tussenconclusie 181
4.4 Beslissen over feiten naar Nederlands strafrecht 183
4.4.1 Bewijsrisicoverdeling 184
4.4.2 Aannemelijke verweren 185
4.4.3 Beslissen over feiten: het bewijsoordeel 193
4.4.3.1 Beslissen over watermerken 193
4.4.3.2 Deskundigen 195
4.4.4 Tussenconclusie 199
4.5 Beslissen over feiten naar Belgisch strafrecht 200
4.5.1 Bewijsrisicoverdeling 201
4.5.2 Meest aannemelijke verweren 202
4.5.3 Beslissen over feiten: het bewijsoordeel 203
4.5.3.1 Beslissen over watermerken 204
4.5.3.2 Deskundigen 205
4.5.4 Tussenconclusie 208
4.6 Samenvatting en conclusie 209

5 De toelaatbaarheid van watermerken als juridisch bewijs 213

5.1 Inleiding 213
5.2 De kwalificatie van watermerken als juridisch bewijsmiddel 215
5.2.1 Civielrechtelijke kwalificatie 215
5.2.1.1 Nederland 215
5.2.1.2 België 216

5.2.2 Strafrechtelijke kwalificatie 217
5.2.2.1 Nederland 217
5.2.2.2 België 218
5.3 Watermerken als (on)rechtmatig verkregen bewijs 219
5.3.1 Grondrechten 220
5.3.1.1 Watermerken in het licht van Europese grondrechten 220
5.3.1.2 Aandacht voor privacy bij de opkomst van watermerken 225
5.3.2 Civielrechtelijke onrechtmatigheid 232
5.3.2.1 Nederland 233
5.3.2.2 België 243
5.3.3 Strafrechtelijke onrechtmatigheid 246
5.3.3.1 Nederland 246
5.3.3.2 België 248
5.4 Gevolgen van onrechtmatig verkregen bewijs voor watermerken 251
5.4.1 Strafrechtelijke sancties op onrechtmatigheid 252
5.4.1.1 Nederland 252
5.4.1.2 België 258
5.4.2 Civielrechtelijke sancties op onrechtmatigheid 263
5.4.2.1 Nederland 264
5.4.2.2 België 277
5.5 Samenvatting en conclusies 282

6 Waarderen van watermerken 289

6.1 Inleiding 289
6.2 Waarderen van forensisch onderzoek: lessen uit ander forensisch bewijs 290
6.2.1 Kwaliteit van het onderzoek 292
6.2.2 Kwaliteit van de onderzoeker 297
6.2.3 Vertaalslag tussen juristen en andere deskundigen 300
6.2.4 Rapporteren over forensisch onderzoek 302
6.2.5 Tussenconclusie 304

6.3 Waarderen van watermerken als bewijsmiddel 305
6.3.1 Valideren van het gehele proces 307
6.3.2 Aandacht voor aannemelijke verweren ten aanzien van de techniek 310
6.4 Valkuilen bij het interpreteren van (betrouwbare) watermerken 314
6.4.1 Het proces van juridisch beslissen over bewijs 317
6.4.2 De invloed van getallen 320
6.5 Het gebruik van statistiek en deskundigen in het recht 324
6.6 Samenvatting en conclusie 332

7 Over watermerken als juridisch bewijsmiddel 335

7.1 Inleiding 335
7.2 Watermerken als technisch bewijsmiddel 336
7.3 Watermerken en het vaststellen van auteursrechtinbreuk 338
7.4 Watermerken als effectief bewijsmiddel in de context van het bewijsrecht 339
7.5 Watermerken als toelaatbaar bewijsmiddel 341
7.6 Watermerken als betrouwbaar bewijsmiddel 345
7.7 Slotakkoord 347
7.7.1 Inpassingstoets: technische output voor juridische input 347
7.7.2 Randvoorwaarden: juridische input voor technische output 348
7.7.3 Valorisatie: waarde van watermerken als bewijsmiddel 350

Summary 353

Lijst van gebruikte afkortingen 365

Literatuurlijst 367

Jurisprudentieregister 391

1 Inleiding

‘Wie denkt dat hij origineel is, heeft niet genoeg gelezen’.[1]

1.1 Digitale watermerken als juridisch bewijsmiddel

Digitaal watermerken (hierna: watermerken) is een techniek om informatie in een digitaal bestand aan te brengen. Vanaf begin jaren negentig is de ontwikkeling van deze techniek gestimuleerd door zowel de Europese Unie in de vorm van onderzoeksubsidies als door de vraag uit de entertainmentindustrie om een bijdrage te leveren aan het verbeteren van de handhaving van het auteursrecht. Met name de laatste jaren is deze technologie volwassen geworden en worden digitale watermerken steeds vaker ingezet.[2] Eén van de toepassingen van watermerken is het zogenoemde ‘traitor tracing’ met behulp van niet-waarneembare watermerken. Deze watermerken beperken de eindgebruiker niet in zijn normale gebruik en kunnen tegelijk de rechthebbende repressieve bescherming bieden.

In dit onderzoek staat de juridische effectiviteit van deze watermerken centraal. Zowel aanbieders van watermerken als particuliere websites, zoals internetfora over bijvoorbeeld fotografie, presenteren digitale watermerken vaak als een betrouwbaar juridisch bewijsmiddel. Watermerken worden al langer ingezet op kleine schaal, zoals bij het verspreiden van films onder juryleden of bij pay-tv in hotels.[3] Gedurende het onderzoek kwam de toepassing van watermerken op een grotere schaal op toen ook e-boeken van watermerken werden voorzien. Bijvoorbeeld bij de e-boeken van Harry Potter. In Nederland voorziet het grote distributie-platform eBoekhuis de meeste van haar e-boeken van een watermerk en zijn over de handhaving daarvan afspraken gemaakt met de stichting BREIN waardoor de kans op handhaving toeneemt.[4] Dit kan het begin zijn van een bredere toepassing van watermerken in bijvoorbeeld audio, films of foto’s.[5] Vanwege deze ontwikkelingen neemt de kans toe dat de effectiviteit van het watermerk als bewijsmiddel in een juridische procedure een rol gaat spelen. In de literatuur over watermerken worden, mede als onderdeel van het weten-schappelijk proces van falsificatie, echter kritische kanttekeningen geplaatst bij diverse water-merksystemen. Deze kritiek wordt veelal benoemd in termen van mogelijke aanvallen die het gebruik of de betrouwbaarheid van het watermerksysteem kunnen aantasten.[6] Eén van de

[1] De bron van de uitspraak is mij onbekend, maar de uitspraak wordt ook wel toegeschreven E.M. Meijers. In vergelijkbare bewoordingen Van Dunne in een interview met AA (1995, p. 764; AA19950764): ‘Je moet nooit denken dat je iets voor het eerst zegt’.
[2] Zie o.m. Pérez Freire 2008 (diss.), p. 6.
[3] Vgl. HvJ 30 september 2010, zaak C-581/08, ECLI:EU:C:2010:559 (EMI Group). Het Hof beschrijft in overweging 10 de werking van watermerken bij CD’s: ‘EMI verstrekt daartoe muziekopnames in verschillende vormen: van een digitaal watermerk voorziene opneembare cd’s voor distributie vóór de release van het album, waarop de naam van de ontvanger staat en waarbij traceerbaar is van wie eventuele kopieën afkomstig zijn.’
[4] http://www.ereaders.nl/09081301_inzet_brein_juridisch_afgedekt_in_nieuw_ebookdistributiecontract.
[5] Hoeveel en waar watermerken in de commerciele wereld precies worden ingezet blijft onduidelijk. Zo meldde Tweakers (28 augutus 2015) dat er een manier was gevonden om de hdcp-beveiliging van 4kstreams van Netflix te omzeilen, maar dat de films ook watermerken bevatten.
[6] Zie o.m. Craver, Yeo & Yeung 1998; Petitcolas, Anderson & Kuhn 1999, p. 1069; Cox e.a. 2008, p. 340.

aanvallen die in de literatuur wordt onderscheiden is de juridische aanval. Hierbij staat de vraag centraal of het watermerk in de rechtszaal als bewijs kan dienen. Deze vraag blijft tot op heden in zowel de technische literatuur als de juridische literatuur verregaand onbesproken. Niettemin is zij van evident belang, omdat de effectiviteit van deze watermerken veelal afhangt van de bruikbaarheid daarvan in rechte. Of een watermerk als een bruikbaar bewijsmiddel kan dienen, hangt niet alleen samen met de (technische) betrouwbaarheid van een watermerksysteem, maar ook met de vraag of het watermerk juridisch toelaatbaar is en hoe het in een juridische procedure zal worden gewaardeerd. Voor die waardering wordt, evenals bij ander forensisch bewijs zoals DNA-bewijs, veelal een beroep gedaan op de kennis van deskundigen waarna een brug moet worden geslagen tussen de (technische) deskundigen en juristen. Hier vindt de wisselwerking plaats tussen de wetenschappelijke disciplines die onderzoek doen naar watermerktechnieken en de juristen die het watermerk een plaats moeten geven in het recht.

In dit onderzoek staat het niet-waarneembare digitale watermerk met een traceerdoel centraal. Hoewel deze watermerken ook een authenticatiedoel kunnen hebben, wordt in dit onderzoek aandacht besteed aan de toepassing ‘tracing’ waarbij gegevens van de licentienemer in een audio-, video- of fotobestand wordt opgenomen met als doel om de licentienemer rechtens aan te kunnen spreken wanneer het bestand zonder toestemming van de rechthebbende op internet is verschenen.

1.2 Probleemstelling en nadere afbakening

Dit onderzoek strekt ertoe om het watermerk als bewijsmiddel in juridisch perspectief te plaatsen. Daarbij is de volgende vraag centraal gesteld:

> Kan een niet-waarneembaar digitaal watermerk dat als doel heeft de licentienemer te traceren, in Nederland een effectief juridisch bewijsmiddel vormen bij de handhaving van inbreuk op auteursrechten op digitaal beschikbaar gestelde foto’s, muziek en video op internet?

Voor de beantwoording van deze vraag is een aantal deelvragen geformuleerd:

1. Wat is een digitaal watermerk en wat kan het technisch bewijzen?
2. Wanneer is er sprake van inbreuk op het auteursrecht en op welke wijze kan het watermerk aan de vaststelling daarvan bijdragen?
3. Wanneer is het watermerk preliminair een effectief bewijsmiddel in de context van het bewijsrecht?
4. Wanneer is het watermerk een toelaatbaar juridisch bewijsmiddel?
5. Wanneer is het watermerk een betrouwbaar bewijsmiddel?

De centrale onderzoeksvraag bestaat uit een aantal elementen die een nadere toelichting vereisen.

Het eerste element betreft de effectiviteit van het watermerk als juridisch bewijsmiddel. Een watermerk wordt als een effectief juridisch bewijsmiddel gezien wanneer de rechter het binnen de bewijsrechtelijke context kan aanvaarden als juridisch bewijsmiddel ter vaststelling van het feit dat het bestand aan de vermeende licentienemer toebehoort.[7] Dat betekent kort gezegd, dat een watermerk effectief is wanneer de rechter tot het oordeel komt dat het watermerk een toelaatbaar en betrouwbaar bewijsmiddel is. De term licentienemer verwijst hier naar degene die de licentie heeft gesloten.[8] Dat betekent dat de rechter het watermerk tenminste als een toelaatbaar en betrouwbaar bewijsmiddel moet kunnen accepteren. Voor de vraag of de licentienemer uiteindelijk aansprakelijk kan worden gehouden voor het plegen van inbreuk op het auteursrecht of naburige recht is meer nodig dan enkel het watermerk als bewijsmiddel. Deze vraag wordt verder dan ook zeer beperkt behandeld. De nadruk ligt op het beantwoorden van de vraag of het watermerk een effectief bewijsmiddel is. Vanuit dat perspectief is het vooral relevant om aandacht te besteden aan de vraag welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren over het te bewijzen feit waarvoor het watermerk wordt aangevoerd en op welke wijze de rechter deze stellingen moet beoordelen. In de praktijk kan juridisch bewijs, kort gezegd, geleverd worden door alle betrouwbare bewijsmiddelen. De vraag naar de juridische kwalificatie van het watermerk als juridisch bewijsmiddel wordt voor de volledigheid dan ook slechts kort behandeld. De nadruk ten aanzien van de toelaatbaarheid van het watermerk als bewijsmiddel ligt op de vraag onder welke omstandigheden het watermerk een toelaatbaar bewijsmiddel vormt en welke sancties denkbaar zijn wanneer dit niet het geval is.

Het tweede element dat een nadere toelichting behoeft is de term handhaving. Meer in het algemeen ziet de term handhaving kort gezegd op het scala aan activiteiten dat normconform gedrag bewerkstelligt.[9] In het licht van de vraagstelling wordt met de term handhaving gedoeld op handhaving met juridische middelen. Het is dan de vraag of het watermerk als juridisch bewijsmiddel er aan kan bijdragen de rechter ervan te overtuigen om de rechthebbende of OM uiteindelijk de gevraagde juridische middelen te verschaffen om het auteursrecht te handhaven.

[7] Zie verder par. 2.2.4 en 3.4.

[8] Het kan gaan om klassieke licentienemers, maar ook om recensenten. Als uitgangspunt geldt dat de rechthebbende of het OM een procedure zal voeren tegen degene die in het watermerk is opgenomen. Tijdens de procedure zal blijken of deze persoon ook daadwerkelijk als 'licentienemer' kan worden gekwalificeerd en of hij in strijd met de contractuele voorwaarden heeft gehandeld door het werk op internet te plaatsen. Wanneer in een procedure komt vast te staan dat de authenticatie onjuist is gebleken of dat het watermerk vals is zal zonder nader bewijs niet meer kunnen worden gesproken van een licentienemer. Vanwege de leesbaarheid is gekozen om de term licentienemer aan te houden in plaats van vermeende licentienemer. Zie verder par. 2.2.5 (authenticatie) en par. 3.4. (auteursrecht). In het licht van het per 13 juni 2014 in werking getreden artikel 7:5 BW; HR 27 april 2012, ECLI:NL:HR:2012:BV1301 (Beeldbrigade) en HvJ EU 3 juli 2012, ECLI:EU:C:2012:407 (UsedSoft) zou de levering van digitale werken, zoals films, foto's en muziek naar Nederlands (en via HvJ EU ook Belgisch) recht mogelijk ook als een consumentenkoop worden gezien. De vragen dit verder met zich meebrengt laat ik verder buiten beschouwing.

[9] Blomberg & Michiels 1997, p. 29; Van Duyne en Kwanten 2004, p. 7.

Het derde element ziet op de behandeling van het auteursrecht. Foto's vinden juridisch hun bescherming in het auteursrecht. Muziek en film kan afhankelijk van de inhoud daarvan zowel bescherming vinden in het auteursrecht als in naburige rechten. Voor het gebruik daarvan is, behoudens de wettelijke beperkingen, toestemming vereist van zowel de auteursrechthebbende als de houder van het naburige recht. Hoewel er verschillen zijn tussen beide rechten, zijn deze voor dit onderzoek verder minder relevant en wordt bij de behandeling van het probandum enkel stilgestaan bij het auteursrecht.[10]

Het vierde element betreft de term internet. Met de term internet wordt verwezen naar publiek toegankelijke internettoepassingen waar gebruikers bestanden met elkaar kunnen uitwisselen.[11]

Omdat in de Nederlandse rechtspraktijk het auteursrecht voornamelijk civielrechtelijk wordt gehandhaafd is het Nederlands civiele bewijsrecht als uitgangspunt genomen. Het perspectief van de rechter staat hierbij centraal.[12] De nadruk zal tevens liggen op de consument als licentienemer. Hoewel meer vragen van invloed kunnen zijn op de effectiviteit van het watermerk is ervoor gekozen de nadruk te leggen op de toelaatbaarheid en waardering van het watermerk.[13]

In dit onderzoek worden de maatschappelijke aanvaardbaarheid van het auteursrecht en de inzet van watermerken ter handhaving van dat auteursrecht als gegeven beschouwd. Het onderhavige onderzoek sluit in die zin aan bij de huidige praktijk, zowel vanuit het oogpunt van de handhaving van het auteursrecht als (inmiddels) vanuit de inzet van de techniek.

Ondanks dat veel IE-procedures in kort geding worden beslist is ervoor gekozen om het watermerk te plaatsen in het kader van het algemene bewijsrecht in eerste aanleg.[14] Ten eerste omdat in zaken waarin technische vragen een belangrijke rol spelen de rechter soms van oordeel is dat de zaak voor behandeling in kort geding feitelijk te complex is.[15] Ten tweede brengt de aard van de kortgedingprocedure met zich mee dat het bewijsrecht in dergelijke procedures geen toepassing kan vinden en aan de kortgedingrechter een grote mate van vrijheid toekomt bij de beoordeling van het bewijs.[16] Een daadwerkelijke inhoudelijke toets zal om die reden plaatsvinden in een bodemprocedure bij de rechter in eerste aanleg, waar het

[10] Zie verder voor Nederland uitgebreid Spoor, Verkade & Visser 2005 en voor België Brison & Vanhees 2012.

[11] Internet is in beginsel niet meer is dan een netwerk van computernetwerken die via verschillende protocollen (bv. http, ftp) communicatie met elkaar mogelijk maken. Waar het in dit onderzoek in de kern om gaat is dat iemand auteursrechtelijk beschermde content via het internet publiek beschikbaar maakt. Voor een nadere omschrijving van computer, internet en recht verwijs ik naar de eerste tweede hoofdstukken van Franken e.a. 2004 en naar het tweede hoofdstuk van Voulon 2010 (diss.).

[12] Dit onderzoek is vanzelfsprekend ook voor de procesdeelnemers van belang. Zij kunnen aan de hand van de te bespreken onderwerpen een gemotiveerd standpunt innemen over de waarde van het watermerk. Als uitgangspunt geldt dat partijen en de rechter oprecht volgens de regels het feit proberen te bewijzen.

[13] Zie o.m. Schum 2009, p. 68: 'In all legal systems known to me there are two major issues concerning evidence: admissibility and proof'.

[14] Zie o.m. Visser (2008, p. 1918) die in zijn onderzoek naar meerdere IE-rechten stelt dat de meeste IE-geschillen in kort geding en in één instantie definitief worden beslist.

[15] Zie o.m. vzr. Rb. Roermond 19 februari 2009, BH2949, ov. 4.2 (More Entertainment/MyP2P); vzr Rb. Amsterdam 22 oktober 2009, BK1067, ov. 5.8 (Brein/Pirate Bay).

[16] Art. 284 Rv; Kamerstukken II 1999/00, 26855, nr. 3, p. 158 (MvT); Asser 2013, p. 25; HR 1 juni 2007 ECLI:NL:HR:2007:BA3525, NJ 2007, 309. Zie voor meer verwijzingen noot 44 in de conclusie van A-G Verkade voor dit arrest.

gewone bewijsrecht van toepassing is. Het is in die procedure waar het watermerk zijn waarde moet bewijzen. Een benadering vanuit het perspectief van eerste aanleg vormt om die reden dan ook het beste uitgangspunt voor dit onderzoek.[17]

Tot slot een opmerking over de beperking die gelegen is in het type onderzoek. Vanwege de verschillende deelonderwerpen die nodig zijn bij het beantwoorden van de vraagstelling wordt niet uitvoerig stilgestaan bij alle relevante onderdelen. Voor deze en andere deelonderwerpen wordt in de voetnoten verwezen naar de andere literatuur.

In dit onderzoek wordt veelvuldig gebruik gemaakt van de termen watermerk, watermerken, watermerktechniek en watermerksysteem. Met deze termen wordt, tenzij anders is aangegeven, het volgende bedoeld. De term 'watermerk' verwijst naar de boodschap die in een signaal (computerbestand) is of wordt aangebracht. Hierbij kan zowel worden gedacht aan verschillende type boodschappen, zoals het verstrekken van informatie over de gebruiker, als aan het bepalen van het gedrag (bv. kopiëren niet toestaan). De term 'watermerken' verwijst naar het meervoud van 'watermerk' of naar het proces van watermerken. De termen 'watermerktechniek' en 'watermerksysteem' verwijzen naar de wijze waarop het watermerk wordt aangebracht in het gastobject. Anders gezegd, watermerktechnieken verwijzen naar methoden om boodschappen te ver- of ontsleutelen. Een watermerksysteem verwijst naar het gehele proces van aanbrengen van een watermerk tot het detecteren ervan, waaronder ook het embedden en detecteren van het watermerk.

1.3 Doel en methode van onderzoek

Dit onderzoek heeft primair tot doel om het watermerk in een juridisch perspectief te plaatsen. Centraal staat de vraag of het watermerk in het Nederlands civiel bewijsrecht kan worden ingepast en of het watermerk een effect bewijsmiddel is.[18] De inpassingstoets functioneert in deze context als een voorvraag. Het watermerk kan immers niet effectief zijn wanneer het niet in het Nederlandse bewijssysteem zou passen. Of het watermerk in dit systeem kan worden ingepast is voornamelijk een vraag naar de toelaatbaarheid van het watermerk.[19] Het antwoord op de vraag of het watermerk een effectief juridisch bewijsmiddel is wordt naast de vorige vraag ook bepaald door het antwoord op de vraag of de rechter het watermerk als een betrouwbaar bewijsmiddel kan aanvaarden.[20]

1.3.1 Onderzoeksmethoden: juridisch-normatief en rechtsvergelijkend onderzoek

Dit onderzoek betreft voornamelijk een juridisch-normatief onderzoek en is uitgevoerd als een desk- en literatuurstudie, waarbij relevante regelgeving, de literatuur en jurisprudentie is

[17] Hiermee wordt het onderwerp afgebakend, maar wordt niet bedoeld dat het bewijsrecht in hoger beroep geheel anders zou zijn. Voor zover relevant zijn ook de appelrechters gehouden tot een zelfstandige bewijswaardering te komen zolang dit binnen de grenzen van de rechtsstrijd valt.
[18] Zie voor een nadere omschrijving van de inpassingstoets o.m. Tijssen 2009 (diss.), p. 74.
[19] De vraag wordt afzonderlijk in hoofdstuk 5 behandeld.
[20] Deze laatste vraag wordt apart behandeld in hoofdstuk 6.

bestudeerd.[21] Waar relevant en beschikbaar zijn ook enkele empirische gegevens verzameld over het down- en uploaden van content en de wijze waarop rechters tot hun beslissing komen. Hiervoor is geen zelfstandig empirisch onderzoek verricht, maar is afgegaan op beschikbare gegevens in de literatuur en te raadplegen openbare rapporten, jaarverslagen en wetenschappelijk onderzoek. Voor de bestudering van watermerken en forensisch digitaal bewijs in het algemeen is eveneens gebruik gemaakt van desk- en literatuuronderzoek.

Vanwege het inpassingsdoel en met het oog op het verkrijgen van een beter inzicht in het Nederlandse civiele recht is gekozen voor rechtsvergelijkend onderzoek. De rechtsvergelijking is met name uitgevoerd om meer inzicht te verkrijgen in het eigen Nederlandse stelsel.[22] Het dient ook als inspiratiebron en bron van kennis.[23] Het object van de rechtsvergelijking is, vanuit een functioneel perspectief, de handhaving van het auteursrecht. Om het Nederlandse recht met enige distantie te kunnen beschouwen, is gekozen voor een externe rechtsvergelijking met één ander land. De beperking tot één land is ingegeven door het gegeven dat de vergelijking zowel het civiele recht als het strafrecht omvat alsmede de wisselwerking daartussen.[24] Daarnaast wordt in dit onderzoek aandacht besteed aan de techniek van watermerken waardoor er gezien de beperkte tijdsduur waarbinnen het onderzoek moet worden verricht keuzes gemaakt zijn in de te behandelen onderwerpen. De Europese dimensie wordt besproken voor zover deze relevant is, zoals bij het auteursrecht en het privacyrecht. Het bewijsrecht, is voor zover het de waardering van watermerken betreft, in zijn geheel niet geharmoniseerd en de bespreking richt zich daar uitsluitend tot het nationale recht.[25]

In het kader van het jurisprudentieonderzoek is voor het Nederlandse recht gebruik gemaakt van rechtspraak.nl, de officiële site van onder meer de rechtbanken, gerechtshoven en de Hoge Raad. Voor het Belgische recht is juridat.be (aangeduid als Juridat) gebruikt, de portaalsite van de Rechterlijke Macht van België.[26] Beide databanken zijn met behulp van de rechterlijke macht opengesteld en zijn in die zin beide een publieke databank wat verificatie van dit onderzoek (eenvoudiger) mogelijk maakt.[27] Juridat wordt als doorzoekbare databank ook wel vergeleken met rechtspraak.nl.[28] Er zijn vooralsnog echter belangrijke verschillen.

[21] Dit wordt ook wel aangeduid als klassiek juridisch onderzoek. Zie o.m. Tijssen 2009 (diss.), p. 161.
[22] Of zoals Bruinsma (2003, p. 17) het verwoordde: 'The best method of getting to know one's own legal system and culture is to compare it with others'.
[23] Zie voor de verschillende doelen van rechtsvergelijking o.m. Zweigert & Kotz 1998, p. 15 ev; Gorlé e.a 2007, p. 16. Zie ook andere onderzoeken in het domein van het bewijsrecht o.m. Giesen 2001 (diss.); Embregts 2003 (diss.); Van Stekelenburg 2009 (diss.); Verkerk 2010 (diss.). In het domein van het auteursrecht zie o.m. Ringnalda, Elferink & De Cock Buning 2009.
[24] Kokkini-Iatridou (1988, p. 139.) beschouwt vier rechtsorders als het maximum voor jonge onderzoekers. Beltzer 2008 (p. 180) raadt het aan voorzichtig te zijn en, ook al schijnt het bon ton te zijn, raadt hij promovendi vrijwel altijd af om vergelijkingen te maken met vergelijkbare rechtsregels in andere landen.
[25] Een enkele bewijsrechtelijke maatregel ten aanzien van het auteursrecht is geregeld in de Handhavingsrichtlijn maar is in deze verder niet relevant.
[26] Rechtspraak.nl is de officiële site van o.m. de Nederlandse rechtbanken, gerechtshoven en de Hoge Raad.
[27] Het Nederlandse rechtspraak.nl heeft ook een samenwerking met de commerciele databank van uitgeverij Kluwer waardoor ook vindplaatsen in bekende juridische tijdschriften zijn terug te vinden.
[28] Zie o.m. http://www.vpod.nl/zoeken-in-belgische-rechtspraak/

Rechtspraak.nl bestaat al veel langer dan Juridat, dat in 2012 is begonnen met het beschikbaar stellen van uitspraken. Dit blijkt ook uit de gegevens die op de websites ter beschikking worden gesteld. Waar erop Juridat nog weinig informatie te vinden is anders dan de uitspraken zelf kent de Nederlandse databank uitgebreide beschrijvingen ten aanzien van het gebruik van de open data en de selectiecriteria alsmede de wijze waarop in verschillende rechtsgebieden en op instantie kan worden gezocht.[29] Daarnaast is rechtspraak.nl in 2013 al overgestapt op de European Case Law Identifier (ECLI), een Europese standaard voor het uniek nummeren van rechterlijke uitspraken.[30] Ook het aantal uitspraken dat is opgenomen lijkt te verschillen. Zo geeft de meest uitgebreide en algemene zoekopdracht met het trefwoord [auteursrecht] bij alle instanties in alle rechtsgebieden in Juridat 200 treffers en op rechtspraak.nl 1332 resultaten.[31] Voorlopig is het ook niet mogelijk om in Juridat volledig automatisch te zoeken omdat arresten ook dubbel in de resultatenlijst worden vertoond, veelal vanwege de taal (Nederlands, Frans, Duits) waarin de arresten (moeten) worden gewezen. Het blijkt in Juridat ook (nog) niet mogelijk om binnen een specifiek rechtsgebied te zoeken, waardoor nog veel handmatig moet worden uitgezocht. Dit heeft ook tot gevolg gehad dat bepaald jurisprudentieonderzoek in Nederland wel heeft plaatsgevonden en in België, vanwege een te kleine dataset, niet. De wijze waarop het jurisprudentieonderzoek is uitgevoerd per deelonderwerp zal in de desbetreffende paragrafen nader worden toegelicht.

Voor de bevindingen is naast raadpleging van relevante regelgeving, jurisprudentie en literatuur ook overleg gevoerd met specialisten en stakeholders in het domein van de handhaving van het auteursrecht, watermerken en digitaal forensisch onderzoek.[32] Aan deze experts en stakeholders zijn algemene vragen gesteld over de mate waarin de theorie van de praktijk verschilt en hoe in de praktijk wordt aangekeken tegen de onderwerpen waar zij als expert of stakeholder veel mee te maken hebben. Tevens zijn waar nodig enkele specifieke vragen voorgelegd om een beter begrip te krijgen van specifieke zaken en het functioneren daarvan in de praktijk. Deze gesprekken dienden ter oriëntatie in het domein van expertise van de betreffende specialisten en ter verificatie en falsificatie van eerder door derden uitgevoerd onderzoek of controle van mijn eigen bevindingen. Hiermee is niet gezegd dat deze experts mijn mening delen. De definitieve tekst is dan ook niet aan hen voorgelegd en komt volledig voor mijn verantwoordelijkheid.

Waar relevant en beschikbaar zijn ook enkele empirische gegevens verzameld uit andere onderzoeken en toegepast op de voorliggende situatie. Daarbij is zoveel mogelijk rekening

[29] http://www.rechtspraak.nl/Uitspraken-en-Registers/Uitspraken/Pages/default.aspx
[30] Het idee is dat alle landen in de EU deze ECLI-nummering gebruiken. De nummering is alsvolgt opgebouwd: ECLI:landcode:gerechtscode:jaar:nummer. De code geeft echter niet aan op welke datum de uitspraak is gedaan.
[31] Laatstelijk uitgevoerd op 1 januari 2014.
[32] Voor digitaal forensisch onderzoek is gesproken met medewerkers van FOX-IT (inclusief summerschool), Ernst & Young (Forensic Technology & Discovery Services); voor watermerken: Technische Universiteit Delft, IBBT, Booxstream, Civolution; voor (onderzoek naar) handhaving van content: Pathe, Kleine filmhuizen, BREIN, BAF, Disney, SEO. Daarnaast is erop verschillende bijeenkomsten of via e-mail ook gesproken met psychologen over bewijsbeslissingen en forensisch onderzoekers over de rol van bewijsvoering en de resultaten van forensisch onderzoek als bewijsmiddel.

gehouden met de beperkingen (de mitsen en maren) die ieder onderzoek met zich meebrengt.[33] Zo is ieder onderzoek beperkt tot een specifieke context, periode, populatie of jurisdictie. Een andere beperking kan gevonden worden in de toepassing van deze onderzoeken in dit onderzoek. Zo is in dit onderzoek onder meer gebruik gemaakt van onderzoeken uit de Verenigde Staten, terwijl niet uitgesloten kan worden dat eenzelfde onderzoek in Nederland en België mogelijk tot andere resultaten zou leiden.[34] Een ieder die de uitkomsten van empirische onderzoeken nader bekijkt zal opvallen dat de onderzoeker(s) veel voorbehouden maken, waardoor de waarde van deze onderzoeken beperkt is. Toch heb ik waarde gehecht aan het gebruik van deze onderzoeken. Zij geven, meer dan de mening van een juridisch auteur, op een wetenschappelijke wijze inzicht in een bepaald onderwerp.

1.3.2 Selectie van een rechtsstelsel

Voor de geografische keuzebepaling bestaan bij rechtsvergelijkend onderzoek geen harde regels.[35] Het zou in dit onderzoek, gezien de harmoniserende werking die uitgaat van Europa, de voorkeur verdienen een land in Europa te kiezen met éénzelfde juridische rechtssysteem en traditie. Een beperkt verkennend onderzoek maakte bij aanvang duidelijk dat er noch in de Verenigde Staten noch in het Verenigd Koninkrijk, Frankrijk of Duitsland in de literatuur of jurisprudentie eerder aandacht is geweest voor watermerken als juridisch bewijsmiddel. Een rechtsvergelijking met deze landen levert in die zin geen meerwaarde op. Daar komt bij dat een algemene rechtsvergelijking met deze landen, ook in het kader van het bewijsrecht, regelmatig voorkomt.[36] Uiteindelijk is gekozen voor België. Deze keuze is ingegeven door drie overwegingen. Ten eerste vanwege de samenwerking met de Vrije Universiteit Brussel binnen dit project met betrekking tot watermerken. Ten tweede de juridische vergelijkbaarheid van het Belgische procedurele systeem met het Nederlandse, waardoor een goede inbedding in het Nederlandse procesrecht kan worden verwezenlijkt en de compatibiliteit met het EVRM en Europees beleid en regelgeving kan worden gewaarborgd.[37] Daarbij speelt mee dat de economische en maatschappelijke ontwikkelingen in beide landen vergelijkbaar zijn, de Benelux veelal een voorloper is geweest voor Europese regelgeving en op het gebied van intellectueel eigendomsrechten er veel samenwerking plaatsvindt, niet in de laatste plaats vanwege de gedeeltelijke overeenstemming in taal. Ten derde is bij de keuze van het rechtsstelsel rekening gehouden met de beschikbaarheid en de toegankelijkheid tot materiaal

[33] Zie voor verschillende beperkingen ten aanzien van empirisch onderzoek ook de verschillende publicaties in Van Boom, Giesen en Verheij 2013 (Capita Civilogie). Zie voor beperkingen ten aanzien van het gebruik van psychologisch onderzoek en bewijswaardering ook Enneking, Giesen & Rijnhout 2013, p. 1021.
[34] Zie ook par. 6.4.
[35] Zweigert & Kötz geven weliswaar vuistregels, maar deze zien vooral op de bestudering van het verbintenissen- en zakenrecht. Zie ook Gorlé e.a. 2007, p. 31. Deze keuze blijft tot op zekere hoogte arbitrair en zal mede afhangen van de voorkennis, vooronderstellingen, praktische overwegingen en subjectieve voorkeuren van de onderzoeker.
[36] Doordat naar deze landen regelmatig rechtsvergelijkend onderzoek wordt gedaan zijn deze landen al grotendeels verkend. Zo heeft Van Stekelenburg 2009 (diss.) een rechtsvergelijkend onderzoek verricht naar de betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht en deed Verkerk 2010 (diss.) onderzoek naar Fact-Finding in Civil Litigation: A Comparative Perspective.
[37] Zie voor het belang daarvan o.m. Adams 2011, p. 196 en de daar aangehaalde literatuur.

(inclusief de taal) en buitenlandse experts.[38] Hoewel er beleidsmatige verschillen bestaan tussen de deelstaten Vlaanderen en Wallonië geldt ten aanzien van het bewijsrecht inzake het auteursrecht federaal recht waardoor een nader onderscheid niet nodig is.[39]

België biedt voor Nederland een interessante vergelijking.[40] Het land staat in taal en (Franse) achtergrond voldoende dichtbij om rechtsvergelijking zinvol te maken. Daarnaast bestaan er ook interessante verschillen, bijvoorbeeld door de daadwerkelijke mogelijkheden om het auteursrecht strafrechtelijk te handhaven. Nederland zou daarnaast een minder formele rechtscultuur hebben en meer gericht zijn op het resultaat.[41] Dit kan tot gevolg hebben dat er een minder strikte houding ten aanzien van grondrechten bestaat waardoor eventuele problemen met bijvoorbeeld privacy worden verhuld. Rechtsvergelijking met een land met een formelere cultuur kan grondrechten op een andere wijze benaderen en zou voor Nederland nieuwe perspectieven kunnen bieden.

1.3.3 Rechtsvergelijking

Rechtsvergelijkend onderzoek wordt in de rechtsvergelijkende literatuur samen met de bijbehorende methoden in verschillende fasen opgedeeld.[42] In de eerste fase wordt het te onderzoeken object geïdentificeerd. De tweede beschrijft de onderzochte rechtsstelsels gevolgd door een derde fase waarin de overeenkomsten en verschillen worden beschreven. Tot slot worden in de vierde fase de onderzochte rechtsstelsels vergeleken en verklaard. Het onderhavige onderzoek heeft niet als primair doel te komen tot een rechtsvergelijking en verklaring, zoals deze in de derde en vierde fase is beoogd. In dit onderzoek staat de beschrijving van het Belgische recht aan de hand van het onderzoeksobject centraal wat overeenkomt met de eerste en tweede fase in het beschreven onderzoeksproces.[43] In de eerste fase is de identificatie van het onderzoeksobject van belang. Het onderzoeksobject vloeit voort uit de centrale onderzoeksvraag en de daaruit voortvloeiende deelvragen. Voor het uitvoeren van de rechtsvergelijking is primair gekozen voor de gebruikelijke functionele

[38] Zie voor de toegankelijkheid van materiaal o.m. Adams 2011, p. 195 en voor de rol van taal o.m. Kramer 2006, p. 254 en de aldaar genoemde verwijzen.
[39] Zie bijvoorbeeld Werkers e.a. 2009 die een studie verrichtte in opdracht van de Vlaamse Gemeenschap naar auteursrecht in de digitale samenleving voor digitalisering, archivering en ontsluiting van culturele content. Voor België is zowel naar Nederlandse als naar Franse literatuur onderzoek verricht. De meest relevante en recente werken zijn echter van Cattoir 2013 en Allemeersch 2007 (diss.). Om die reden wordt dan ook het meeste verwezen naar deze Nederlandstalige werken.
[40] Opvallend genoeg heb ik ook bij de Vereniging voor de vergelijkende studie van het recht van België en Nederland geen uitgebreide literatuur gevonden over de vraag waarom een rechtsvergelijking interessant zou zijn. Kennelijk is dat sinds 1947 een gegeven en gezien de publicaties van de vereniging nog steeds actueel.
[41] 'Legal practitioners in the Netherlands handle law less formally and are more result-oriented than their colleagues elsewhere. In doing so they conform to the prevailing authority style that relies on expert opinion' (Bruinsma 2003, p. 18).
[42] De hier gebruikte indeling is ontleend aan: Adams 2011.
[43] Binnen het domein van de rechtsvergelijking wordt dan ook wel gesproken over Auslandkunde. Er is in de titel van deze paragraaf gekozen voor de term rechtsvergelijking omdat deze term naar mijn mening breder bekend is en een inleiding tot doel heeft de lezer een beter begrip te geven van het onderzoek.

methode.[44] Deze methode concentreert zich op de wijze waarop concrete problemen in een ander rechtsstelsel worden opgelost en heeft als voornaamste doel inzichten te verkrijgen om bij te dragen aan de reflectie en ontwikkeling van het Nederlandse recht.[45] Een vergelijking zal dan veelal worden gemaakt op het niveau van de rechtsregel.[46] Om rechtsvergelijking mogelijk te maken is het van belang aandacht te hebben voor zowel de rechtsregels als de bredere context waarbinnen het recht zich afspeelt.[47] Daarbij zijn de volgende regels in acht genomen.[48] De termen en begrippen worden bestudeerd zoals deze worden geïnterpreteerd in de rechtspraktijk. De nationale hiërarchie van originele bronnen wordt daarbij in acht genomen. Voor de vergelijking is het tevens van belang dat de termen en begrippen in haar totaliteit worden beoordeeld. Om die reden zal voor de vergelijking zoveel en compact mogelijk de (afwijkende) context binnen het rechtstelsel worden weergegeven. Voor de rechtsvinding is het bijvoorbeeld van belang dat België, in tegenstelling tot Nederland een constitutioneel Hof heeft en grondrechten daar een grotere invloed op het privaatrecht hebben. Voor een nadere context wordt in voetnoten verwezen naar literatuur. Gezocht is naar de wijze waarop in België het watermerk door de rechter als bewijsmiddel gebruikt zou kunnen worden ter vaststelling van een auteursrechtelijke relevant feit. Een vergelijking zoals bedoeld in de derde fase waarin gekeken wordt naar de overeenkomsten en de verschillen komt slechts aan de orde voor zover zij een alternatief of interessant aanknopingspunt vormt met het oog op de conclusie.

1.4 Verantwoording

1.4.1 Onderzoekskader: IM-PACT-project

De aanleiding van dit onderzoek wordt in de kern gevormd door het IM-PACT-project dat een reeks interdisciplinaire onderzoeken omvat naar de ontsluiting van beeld- en geluidsmateriaal.[49] Het onderhavige onderzoek maakt onderdeel uit van het zogeheten Davinci-project waarin vragen rondom de juridische aspecten van DRM (Digital Rights Management) en technische aspecten van IPMP (Intellectual Property Management & Protection) het sluitstuk vormen het IM-PACT-project. In samenwerking met IBBT-ICTRO

[44] Zie inhoudelijk Zweigert & Kötz 1998, p. 34; Gorlé e.a. 2007, p. 32. Adams 2011, p. 195. Zie voor vergelijkbare onderzoeken o.m. Giesen 2001 (diss.), In de behandeling van de verschillende onderwerpen en de volgorde daarvan is aansluiting gezocht bij het juridisch-normatieve deel van dit onderzoek naar het bewijsrecht in Nederland.
[45] Zie o.m. Zweigert & Kotz 1998, p. 15; Gorlé ea. 2007, p. 32.
[46] Zie o.m. Ancel 1971, p. 99; Kokkini-Iatridou 1988, p. 137.
[47] De specifiek omstandigheden van een land spelen daarbij een belangrijke rol. Rechtsvergelijking vereist dan ook aandacht voor de inbedding van de betreffende rechtsregel in de maatschappelijke structuur, de politieke context en de juridische traditie waarbinnen het recht zijn gelding heeft. Juridische begrippen functioneren samenvattend binnen de context van een bepaald (rechts)systeem. Zie o.m. Termorshuizen-Arts 2003(diss.), p. 20-21; Beltzer 2008 p. 180.
[48] Zie ook Zweigert & Kotz 1998, p. 16; Gorlé e.a. 2007, p. 32.
[49] Het Internationaal Media Pact (IM-Pact) is een gezamenlijk onderzoeksprogramma van het Vlaamse IBBT (Interdisciplinair Instituut voor BreedBandTechnologie) en het Nederlandse ICTRegie (het Nationaal regieorgaan voor ICT-onderzoek en -innovatie) op het gebied van digitale media en bestaat in totaal uit acht interdisciplinaire onderzoeken op het gebied van ontsluiting van beeld- en geluidsmateriaal.

(Vrije Universiteit Brussel) is gezocht naar een technische oplossing voor het ontsluiten van digitale content via het toevoegen van verborgen informatie aan content door middel van watermerken voor de controle van intellectuele eigendomsrechten.[50] Het uitgangspunt van deze onderzoeken is niet om het watermerk te presenteren als de oplossing voor handhavingsproblemen in het auteursrecht, maar om een oplossing te vinden teneinde bezwaren van rechthebbenden tegen het digitaal ter beschikking stellen van materiaal weg te nemen.[51] Voor het bereiken van dit doel moeten zowel juridische als technische barrières overwonnen worden. Het onderhavige onderzoek concentreert zich op de juridische aspecten van watermerken. Tegen deze achtergrond is ervoor gekozen om bij het formuleren van de hoofdvraag aan te sluiten op de vraag uit de praktijk of kort gezegd een niet-waarneembaar digitaal watermerk een effectief juridisch bewijsmiddel kan vormen bij de handhaving van inbreuk op auteursrecht op digitaal beschikbaar gestelde foto's, muziek en video op internet. Daarmee past het onderzoek in meer algemene termen in de thematische profilering in termen van de Europese grand challenges (Inclusive, innovative and secure societies), de nationale topsectoren (High Tech en de Creatieve industrie) en de maatschappelijke impact (valorisatie).[52]

Watermerken vormen sinds de jaren negentig een actief onderzoeksdomein dat bij aanvang van dit onderzoek in 2009 tot een volwassen technisch systeem is geëvolueerd en in de praktijk wordt toegepast.[53] De relevantie van dit onderzoek is tweeledig. Ten eerste is de juridische aanval op watermerken in de wetenschappelijke watermerkliteratuur al vroeg onderkend maar verder nooit onderzocht.[54] Ten tweede worden watermerken zowel door aanbieders als door particuliere websites vaak gepresenteerd als een juridisch bewijsmiddel, waarbij de gedachte is dat het een goed bewijsmiddel zou vormen.[55] De vraag of dit daadwerkelijk zo is blijft tot nu toe onbeantwoord. De relevantie hiervan is recent duidelijk geworden nadat J.K. Rowling haar Harry Potter E-boeken van zowel waarneembare als niet-waarneembare digitale watermerken heeft voorzien en één exemplaar daarvan op internet is verschenen. Het is waarschijnlijk dat er juridische acties zullen volgen en daarmee is de

[50] Zie o.m. de studie in Vlaanderen van Werkers (e.a. 2009, p. 3, 163), die o.m. de maatschappelijke ontwikkelingen, beleidsinitiatieven en het huidige regelgevende kader betreffende digitalisering, archivering en ontsluiting van culturele content in kaart bracht. En in Nederland in het boekblad Dessing 2012 over verhuur van e-boeken, waarbij voor de beveiliging o.m. watermerken een rol spelen.

[51] Zie voor dit belang ook Guibault e.a. 2007, p. 15 en bijv. J.K. Rowling had al eerder bekend gemaakt dat zij afzag van E-boeken vanwege het kopieergevaar. Alle grote filmcontracten bevatten bepalingen omtrent maatregelen die genomen moeten worden inzake de beveiliging van de content van aanschaf tot eindgebruiker. Dat de oplossing van dat probleem meerdere dimensies kent is inmiddels wel duidelijk. Zie o.m. Lessig 1999. Voor meer aspecten van de handhavingsdiscussie o.m. Schermer & Wubben 2011 (Feiten om te delen).

[52] Zie voor verantwoording in die termen ook Stolker 2011, p. 38.

[53] Pérez Freire 2008 (diss., p. 6) geeft ook aan dat algemeen gebruik op grote schaal van technologie in het algemeen pas mogelijk is na twee stappen. Ten eerste een voldoende mate van volwassenheid van de technologie en ten tweede een standaardisatieproces . Watermerken hebben volgens hem de eerste stap gezet.

[54] Zie o.m. Craver 1998, p. 48; Nikolaidis e.a. 2001, p. 994. Met uitzondering van Schellekens 2010 in een artikel in het kader van dit project.

[55] Zie o.m.; http://www.semarang.nl/omgaan_met_foto/watermerk_foto.html; http://ezinearticles.com/?Why-You-Need-To-Place-Watermarks-On-Images-You-Post-Online&id=6967135; http://www.digitalwatermarkingalliance.org/app_forensics.asp.

juridische relevantie direct zichtbaar geworden.[56] Inmiddels heeft in Nederland ook het grote distributieplatform eBoekhuis de meeste van haar eboeken van een watermerk voorzien en zijn over de handhaving daarvan afspraken gemaakt met de stichting BREIN.[57] Onduidelijk is welke watermerktechnieken worden gebruikt. Het grote verschil is gelegen in de waardering van de watermerken. Voor de beantwoording van de juridische vragen maakt de inzet van deze watermerken in beginsel geen noemenswaardig verschil.

Dit onderzoek is daarmee zowel van belang voor de verdere ontwikkeling van de techniek van watermerken als voor juristen die in de toekomst (steeds) vaker met forensisch digitaal bewijs, zoals watermerken, geconfronteerd zullen worden. In het bewijsrecht is er de laatste jaren in een toenemende mate aandacht voor forensisch bewijs. Met name in de literatuur met betrekking tot DNA-bewijs is er verschillende keren gewezen op de kloof tussen de deskundige en de jurist. Dat deze kloof niet alleen bestaat in zaken waarbij DNA-bewijs een rol speelt, maar ook bij ICT-gerelateerde zaken blijkt inmiddels ook uit de literatuur.[58] Ook onderzoek binnen het domein van watermerken gaan (technische) wetenschappers niet altijd uit van een juiste dan wel volledige opvatting van juridische concepten in het recht.[59] Terecht wordt er vanuit deskundigen, vooral uit de hoek van DNA-onderzoek, gepleit voor meer inzicht in en begrip voor de gehanteerde techniek. Het belang daarvan mag ook blijken uit het in 2012 door NWO van start gegane multidisciplinaire programma ‘forensic science’ en de KNAW themabijeenkomst ‘Bèta in crime’ (2012) die tot doel hadden de verschillende disciplines die zich bezighouden met technisch bewijs met elkaar in contact te brengen om daarmee bij te kunnen dragen aan het vergroten van wederzijds inzicht in en begrip voor de verschillende schakels en daarmee bij te dragen aan de discussie rondom technisch bewijs.[60]

1.4.2 Verslag van de onderzoeksbevindingen

Gedurende het onderzoek hebben zich in het bijzonder twee ontwikkelingen voorgedaan die van invloed zijn op de weergave van de hier gepresenteerde onderzoeksbevindingen.

Een eerste ontwikkeling die uiteindelijk van invloed is geweest op het onderzoek en het verslag daarvan betreft de inzet van watermerken. Bij aanvang van dit onderzoek was het onze verwachting dat watermerken mede vanwege de goede mogelijkheden om het te

[56] Inhoudelijk is de (rechts)zaak lastig te volgen omdat uitgeverij Pottermore verder niet bereikbaar was voor commentaar in deze kwestie.
[57] http://www.ereaders.nl/09081301_inzet_brein_juridisch_afgedekt_in_nieuw_ebookdistributiecontract. De rechtmatigheid van deze wijze van handhaven is ook besproken in de Tweede Kamer (Handelingen II, 116).
[58] Zie voor literatuurverwijzingen par. 4.6.4. en het op 11 juni 2012 door de KNAW georganiseerde symposium Bèta in crime, over wetenschappelijk bewijs in rechtszaken waar sprekers met een achtergrond in de bètawetenschappen in gingen op barrières op het pad van technisch bewijs.
[59] Zie bijvoorbeeld Pérez Freire (diss., 2008, p. 5) die in de aanleiding van zijn onderzoek naar Digital Watermarking Security, wetenschappelijk bewijs in de VS op grond van United States vs. Kilgus 1978 (met in de voetnoot een verwijzing naar Daubert (1993)), alleen toelaatbaar acht “if the used techniques are commonly accepted by the scientific community”. Terwijl de toelaatbaarheid en waardering in de VS inmiddels (en ook in 2008) bij de rechter ligt en niet langer in de academische gemeenschap. Zie daarvoor o.m. De Bock 2010, p. 329; Beecher-Monas 2007 (zie o.m. p. 36, 84).
[60] KNAW, Bèta in crime. Wetenschappelijk bewijs in rechtszaken. Symposium, 11 juni 2012.

verbergen in bestanden, zoals muziek, video en foto's zich snel in die sectoren zou ontwikkelen. Om die reden zijn e-boeken en e-games als gastobject van het watermerk buiten het onderzoek gelaten. Tegen het einde van dit onderzoek werd duidelijk dat watermerken op grote schaal ingezet zouden gaan worden bij e-boeken, onder meer doordat J.K. Rowling aankondigden watermerken te gaan gebruiken voor de bescherming van haar e-boeken van Harry Potter.[61] Enige tijd later kondigde ook het Centraal Boekhuis aan haar e-boeken op die wijze te gaan beschermen. De toepassing van watermerken voor e-boeken of games verschilt in beginsel niet van de wijze waarop watermerken in het onderzoek aanvankelijk waren gepresenteerd. Het belangrijkste verschil zit in de toe te passen watermerktechnieken en daarmee op de wijze waarop de verschillende eigenschappen van het watermerk kunnen worden ingezet en welke aanvallen aannemelijk zijn bij e-boeken of e-games. Om het onderzoek meer toepasbaar te maken is bij het beschrijven van de verschillende bevindingen ervoor gekozen om alsnog enkele observaties ten aanzien van het watermerken van e-boeken op te nemen. Hiermee kan het onderzoek bijdragen aan de mogelijke juridische en maatschappelijke discussie over de inzet van watermerken als bewijs- en handhavingsmiddel van het auteursrecht. Door de brede inzet van watermerken in e-boeken is de kans toegenomen dat watermerken een rol gaan spelen in de rechtspraktijk.

Een tweede ontwikkeling die van invloed is op de verslaglegging is de rol die het Nederlandse strafrecht speelt ten aanzien van de handhaving van het auteursrecht van individuele uploaders in Nederland.

Bij de aanvang van het onderzoek in 2009 leek het Nederlandse strafrecht een belangrijke rol te kunnen gaan spelen bij de handhaving van het auteursrecht. Tegen het einde van het onderzoek werd duidelijk dat het strafrecht in Nederland juridisch geen rol speelt of in de nabije toekomst gaat spelen bij de handhaving van het auteursrecht ten aanzien van individuele uploaders.[62] In het licht van deze conclusie (zie hoofdstuk 3) is de vraag opgekomen of het reeds verrichte onderzoek naar het Nederlandse strafrecht moet worden opgenomen in het eindverslag. Tegen de achtergrond van de vraagstelling lijkt er inhoudelijk weinig reden om het strafrecht op te nemen. De hier gebruikte functionele rechtsvergelijkende methode, waarbij de handhaving van het auteursrecht als object centraal staat, schrijft dan voor dat in Nederland de civielrechtelijke handhaving wordt behandeld en in België zowel de civielrechtelijke als de strafrechtelijke handhaving. Anders dan in België, hanteert de Nederlandse overheid al enige jaren als uitgangspunt dat het auteursrecht bij voorkeur civielrechtelijk dient te worden gehandhaafd en dat het strafrecht slechts als ultimum

[61] Zie ook de inzet van watermerken bij games. http://games.slashdot.org/story/12/09/11/149228/activision-blizzard-secretly-watermarking-world-of-warcraft-users;
http://www.gameinformer.com/b/news/archive/2013/02/26/eidos-president-next-xbox-uses-watermarked-discs.aspx

[62] Dit heeft o.m. te maken met een verandert speelveld in de markt en de politiek, zie daarvoor paragraaf 3.3. De uitspraak van HvJ EU 10 april 2014, zaak C-435/12 inzake ACI Adam e.a. tegen Stichting De Thuiskopie waarin het Hof kort gezegd duidelijk maakt dat het maken van privé-kopie uit een ongeoorloofde bron niet is toegestaan (downloaden uit illegale bron), maakt dit niet anders.

remedium dient.[63] Mede door de Aanwijzing intellectuele-eigendomsfraude van het College van procureurs-generaal is strafrechtelijke handhaving van het auteursrecht voor individuele uploaders en personen die niet op grote schaal inbreuk maken, in de praktijk vrijwel uitgesloten.[64] Hiermee is niet gezegd dat (een beperkte) inzet van het strafrecht niet wenselijk zou kunnen zijn. In de literatuur zijn echter geen aanwijzingen te vinden dat strafrechtelijke handhaving effectiever zou zijn of in Nederland anderszins wenselijk zou zijn.[65] Daarnaast heeft het bewijsrecht in strafzaken praktisch geen relevantie voor het bewijsrecht in civiele zaken.[66] Het strafrecht heeft andere doelstellingen en functioneert daardoor ook op een geheel andere wijze. Dat is anders voor het Belgische strafrecht. Daar speelt het strafrecht zowel een rol bij de handhaving van het auteursrecht als in het civiele bewijsrecht vanwege de invloed van het leerstuk van de onrechtmatige verkrijging van bewijsmateriaal in het civiele recht. Daar staat tegenover dat het niet opnemen van het Nederlandse strafrecht als consequentie heeft dat de opgedane kennis niet kenbaar wordt. Dit tegen de achtergrond dat er tot op heden beperkt aandacht is voor de beoordeling van digitaal forensisch bewijs in het strafrechtelijk onderzoek.[67] Bovendien worden met het opnemen van het strafrecht alle handhavings-mogelijkheden die de Auteurswet biedt behandeld. Het verslag biedt daarmee een vollediger beeld van de effectiviteit van het watermerk als juridisch bewijsmiddel dan wanneer enkel het civiele recht zou worden behandeld. Een dergelijke benadering sluit, tegen de achtergrond dat veel juridisch onderzoek ook als naslagwerk wordt gebruikt, ook beter aan bij de valorisatie-eisen die aan onderzoek worden gesteld. Hoewel er naar aanleiding van de vraagstelling geen directe reden is om het Nederlandse strafrecht in het kader van dit onderzoek op te nemen is er, vanwege de kennisdisseminatie en de mogelijkheden die dat biedt voor ander onderzoek, uiteindelijk toch voor gekozen om het Nederlandse strafrecht wel mee te nemen in de verslaglegging.

[63] Zie o.m. Speerpuntenbrief auteursrecht 20©20, 11 april 2011 en verder paragraaf. 3.3.

[64] Aanwijzing intellectuele-eigendomsfraude (2005A022) van het College van procureurs-generaal, Stc. 9 januari 2006, nr. 6, pag. 10 (laatstelijk verlengd tot 31-01-2016; Stc 2010, nr. 1021), nr. 1. Zie verder in het bijzonder het Hof 's-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010: BO8237 (e-donkey) en meer recent het hof Den Haag (27 januari 2014, ECLI:NL:GHDHA:2014:84) verklaarde het OM op deze grond niet-ontvankelijk in de vervolging van een uploader 5000 e-books.

[65] Zie o.m. Deene & Van der Perre 2005, p. 885, die het naar Belgisch recht betreurenswaardig vinden dat 'het auteursrecht meer en meer in een strafrechtelijk moeras verzinkt'. Met name ten aanzien van het strafbaar stellen van downloaden is veel onderzoek verricht (zie o.m. Schermer & Wubben 2011). In dat kader wordt er vooral gewezen op de proportionaliteit en de druk die het strafbaar stellen van invoering daarvan zou hebben op het justitieel apparaat. Bovendien wijzen enkele onderzoeken er daar op dat de inzet van het strafrecht enkel effect heeft als het ook daadwerkelijk wordt gehandhaafd. En daarvoor is een grote capaciteit van de politie en OM nodig die enkel ter beschikking wordt gesteld wanneer de maatschappelijke opvatting over het auteursrecht drastisch veranderd. Verder blijkt in het buitenland niet dat het effect van strafrechtelijke handhaving op lange termijn beter werkt. Ook de beruchte (straf-bestuursrechtelijke) Hadopi-wetgeving in Frankrijk is inmiddels teruggetrokken (10 juli 2013).

[66] De opzet van dit onderzoek laat dan ook geen ruimte voor een interne rechtsvergelijking. Zie voor de mogelijkheden en moeilijkheden ten aanzien van een interne rechtsvergelijking: Nijboer, Schuurmans & Asser 2010.

[67] Een ander argument dat voor de opnemen van het strafrecht pleit is dat de maatschappelijke opvatting in de toekomst kan veranderen waardoor de inzet van het strafrecht wel voor de hand zou komen te liggen. Dit argument geldt voor zoveel onderwerpen dat er weinig reden is om dat argument als doorslaggevend aan te nemen.

Op 10 april 2014 heeft het Hof van Justitie EU arrest gewezen inzake ACI Adam e.a. tegen Stichting De Thuiskopie waarin het Hof, kort gezegd, het maken van privé-kopie uit een ongeoorloofde bron niet toestaat (downloaden uit illegale bron). Hiermee is in theorie de reikwijdte van het watermerk als bewijsmiddel toegenomen.[68] Het watermerk kan dan niet enkel als bewijsmiddel worden gebruikt door rechthebbende om de licentienemer op te sporen die het werk heeft verspreid, maar ook door de licentienemer om aan te tonen dat hij wel over een licentie beschikt en het werk niet illegaal heeft gedownload. Deze laatste situatie is verder niet beschreven in dit onderzoek.

Ten slotte nog een opmerking over het gebruik van hyperlinks in voetnoten. Om ruimte te besparen is niet achter iedere hyperlink een datum aangegeven waarop deze het laatst is geraadpleegd. Bij de laatste herziening van het verslag, eind februari 2015 zijn alle hyperlinks geraadpleegd, tenzij anders is aangegeven.

1.4.3 Taalkeuze: lingua franca of onderzoeksratio

Tot slot wil ik nog een korte opmerking maken over het gebruik van de Nederlandse taal, omdat de wetenschap in het algemeen internationaal georiënteerd is en de lingua franca Engels is. Wetenschappers moeten volgens het KNAW hun werktaal dan ook blijven kiezen op grond van het onderwerp en de context. De commissie Smits heeft voor rechtsgeleerd onderzoek geconcludeerd dat afhankelijk van het thema, rechtsgebied en de doelgroep, het Nederlands naast het Engels een forumtaal is.[69] Ik zal mijn keuze nader toelichten. Allereerst is het van belang vast te stellen dat het Nederlandse recht een vertrekpunt is voor het onderzoek. Dat is op zich nog geen doorslaggevende reden om het Nederlands als onderzoekstaal te gebruiken. Het onderzoek wordt gevormd door de onderzoeksvraag en deze is in de kern genomen nationaal van aard, ook wanneer dit wordt gezien in het licht van de internationale ontwikkelingen.[70] Nu er in dit onderzoek een rechtsvergelijking plaatsvindt met België en het gebruik van de Nederlandse taal mogelijk is, ligt dit mede in het licht van de rechtsvergelijking het meest voor de hand. Om de onderzoeksresultaten ook in de watermerkliteratuur kenbaar te maken is gekozen voor een Engelstalige samenvatting.

1.5 Plan van behandeling

In dit onderzoek staat de meer praktische vraag centraal of een niet-waarneembaar digitaal watermerk dat als doel heeft de licentienemer te traceren, in Nederland een effectief juridisch bewijsmiddel kan vormen bij de handhaving van inbreuk op auteursrecht op digitaal beschikbaar gestelde foto's, muziek en video op internet.[71] In dit verslag wordt deze hoofdvraag als uitgangspunt genomen en wordt stap voor stap gekeken wat het watermerk

[68] HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie).
[69] Daarnaast is er in de literatuur vaker op gewezen dat de publicatie vorm vaak nationaal is. Zie o.m. Tijssen 2009, p. 34; Stolker 2011, p. 29.
[70] Zie ook Stolker (2011, p. 18) over rechtswetenschappelijk onderzoek na de Commissie Koers.
[71] Zie par. 1.4.1.

precies kan bewijzen. In hoofdstuk 2 en 3 wordt eerst onderzocht wat het watermerk technisch en juridisch precies kan bewijzen. De voorlopige conclusie die uit deze hoofdstukken wordt getrokken is dat een betrouwbaar watermerk een verband kan leggen tussen het op internet aangetroffen bestand en de licentienemer, maar geen bewijs kan leveren dat de licentienemer inbreuk heeft gemaakt op het auteursrecht van de rechthebbende. Om die conclusie te kunnen trekken is meer nodig. In de volgende hoofdstukken wordt dat gegeven als uitgangspunt genomen en wordt nagegaan of met behulp van het watermerk ook juridisch een verband kan worden worden gelegd tussen het op internet aangetroffen bestand en de licentienemer.

Een nadere toelichting per hoofdstuk volgt hieronder.

In hoofdstuk twee staat het watermerk als techniek centraal. Allereerst wordt de techniek van watermerken geïntroduceerd door achtereenvolgens in te gaan op de geschiedenis van het watermerk, de classificering van watermerken, de verschillende toepassingen, de techniek van watermerken en de wijze waarop de licentienemer geauthenticeerd dient te worden. Na deze introductie wordt het watermerk voorgesteld als een proces. Dit proces geeft inzicht in de wijze waarop het watermerk wordt aangebracht, verspreid, gedetecteerd en geïnterpreteerd. Afhankelijk van de toepassing van het watermerk wordt gebruik gemaakt van verschillende eigenschappen van deze techniek. De inzet van verschillende eigenschappen speelt vervolgens een belangrijke rol bij het bepalen van de mate van betrouwbaarheid en wordt om die reden dan ook apart behandeld. Aan het einde van het hoofdstuk worden de meest aannemelijke (technische) aanvallen op watermerken besproken.

Hoofdstuk drie gaat in op de vraag of, en zo ja, op welke wijze het watermerk als bewijsmiddel kan bijdragen aan de handhaving van het auteursrecht. Om als bewijsmiddel te kunnen dienen wordt eerst nagegaan of gebruikers het watermerk als techniek zullen accepteren. Daarna is er aandacht voor de vraag of en op welke wijze het watermerk past binnen het huidige handhavingsbeleid. Daartoe wordt het handhavingsbeleid van zowel de overheid als de particulier nader onderzocht door na te gaan welke regiems van toepassing zijn en welk beleid er wordt gevoerd. Vervolgens wordt gekeken naar de vraag wanneer er sprake is van inbreuk op het auteursrecht, welke sancties mogelijk zijn en voor welke elementen het watermerk als bewijs kan dienen. Tot slot wordt aandacht besteed aan de juridische bescherming van watermerken. Daarbij is de vraag of watermerken een technische voorziening vormen die recht geeft op juridische bescherming.

Het watermerk wordt in dit onderzoek als een effectief juridisch bewijsmiddel gezien wanneer de rechter het binnen de bewijsrechtelijke context kan aanvaarden als juridisch bewijsmiddel ter vaststelling van het feit dat het bestand aan de licentienemer toebehoort. Om de effectiviteit van het watermerk te kunnen onderzoeken wordt in hoofdstuk vier gekeken hoe het bewijsrecht werkt op de punten die voor de waardering van watermerken van belang zijn. Vanuit dat perspectief wordt in dit hoofdstuk aandacht besteed aan de vraag welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren over het te bewijzen feit waarvoor

het watermerk wordt aangevoerd en op welke wijze de rechter deze stellingen moet beoordelen. De twee meest aannemelijke verweren, namelijk ten aanzien van de toelaatbaarheid en betrouwbaarheid, die direct de effectiviteit van het watermerk raken worden in de navolgende hoofdstukken nader uitgewerkt.

In hoofdstuk vijf staat de vraag centraal of het watermerk een toelaatbaar bewijsmiddel kan vormen. Voor het beantwoorden van deze vraag is het van belang te bepalen of het watermerk een wettig bewijsmiddel vormt. Vervolgens wordt rechtmatigheid van het bewijsmiddel besproken en wordt gekeken naar de vraag of eventuele onrechtmatigheden in het proces van watermerken gevolgen heeft voor het watermerk als bewijsmiddel.

In hoofdstuk zes staat de waardering van het watermerk centraal. Het watermerk zal in juridische procedures veelal door de rechthebbende als bewijs worden ingebracht in de vorm van een verslag. Om dat verslag te kunnen beoordelen wordt in dit hoofdstuk gekeken naar de vraag welke lessen er kunnen worden getrokken uit andere forensisch bewijs en welke specifiek onderwerpen het verslag tenminste zal moeten beschrijven om er enige bewijskracht aan toe te kennen. Daarna wordt gekeken naar de (psychologische) valkuilen bij het interpreteren van in beginsel betrouwbare watermerken. Tot slot is tegen de achtergrond van de strafzaak tegen Lucia de B., gekeken naar het gebruik van statistiek en deskundigen in het recht.

In hoofdstuk zeven wordt het onderzoek afgesloten met een samenvatting en een conclusie met betrekking tot de centrale hoofdvraag van dit onderzoek.

Dit onderzoek is afgesloten op 1 maart 2015. Ontwikkelingen na deze datum zijn, op een enkele uitzondering na, niet meegenomen in het verslag.

2 Watermerken als technisch bewijsmiddel

'Why Watermarking is Nonsense'.[1]

2.1 Inleiding

Om te kunnen beoordelen of een digitaal watermerk als juridisch bewijsmiddel kan dienen wordt in dit hoofdstuk de techniek van watermerken beschreven. Dit hoofdstuk beoogt geen uitputtende beschrijving te geven over watermerken maar beperkt zich tot een uitleg die noodzakelijk is om de vraag te kunnen beantwoorden of deze techniek in het recht kan worden ingepast en hoe deze gewaardeerd kan worden.[2] In dit onderzoek staan in het bijzonder watermerktechnieken centraal die als doel hebben om de licentienemer na overtreding van het auteursrecht te kunnen traceren. Deze toepassing staat in de watermerkliteratuur bekend als (traitor) tracing.[3] Het domein van watermerken bestaat uiteindelijk uit verschillende disciplines, waardoor het voor een buitenstaander (gemiddelde jurist) lastig is om grip te krijgen op dit fenomeen.[4]

De techniek van watermerken wordt hieronder eerst geintroduceerd door een korte beschrijving van de geschiedenis, classificatie van de techniek en de verschillende toepassingen van watermerken (par. 2.2). In de daarop volgende paragraaf wordt het proces van watermerken uiteengezet van het watermerk tot aan de interpretatie daarvan (par. 2.3). Dit maakt het mogelijk om beter inzicht te geven in de wijze waarop watermerksystemen werken en verschillende onderdelen een plaats te geven. Daarna worden eigenschapppen van watermerksystemen besproken (par. 2.4). Watermerken kunnen voor verschillende toepassingen worden gebruikt. De gekozen toepassing bepaalt in belangrijke mate de eigenschappen waarvan gebruik wordt gemaakt bij het watermerken van een bepaald object. De wisselwerking tussen de gekozen toepassing en de gebruikte eigenschappen alsmede de trade-off tussen de eigenschappen zelf speelt niet alleen een belangrijke rol bij het ontwikkelen van watermerken maar ook voor de betrouwbaarheid ervan. Naast de verschillende keuzen bij de inzet van watermerken wordt de betrouwbaarheid ervan ook voor een belangrijk deel bepaald door de zogenoemde aanvallen die mogelijk zijn op het systeem (par. 2.5). Het hoofdstuk wordt afgesloten met een samenvatting (par. 2.6).

---

[1] Titel van een artikel van C. Herley (2000) waarin hij zijn kritiek deelde over het gebruik van watermerken.

[2] Dit hoofdstuk beperkt zich tot de basis van watermerkensystemen. Zie ter vergelijking Cox e.a. 2008 (p. xxi) die in hun boek over digitale watermerken meer dan 500 pagina's en 22 watermerksystemen gebruiken om de verschillen aspecten van watermerktechnieken uit te leggen. Dit verklaart eveneens waarom de literatuur relatief oud is. De meer recente literatuur betreft vooral zeer specifieke aspecten van watermerken, terwijl er juist in oude literatuur meer aandacht is voor de werking van watermerken.

[3] De term traitor tracing is normatief geladen en juridisch gezien ongelukkig gekozen omdat de term zelf al een inbreukmaker impliceert terwijl het in juridische zin maar de vraag is of de rechter op grond van deze techniek iemand kan aanwijzen.

[4] De complexiteit van dit domein en de noodzaak voor het inroepen van de nodige expertise zal voor de gemiddelde jurist onmiddellijk duidelijk worden wanneer hij in google scholar, de term 'watermarking' of 'watermarking traitor tracing' intikt en enkele documenten die dan verschijnen gaat lezen. De auteur van dit boek is dan ook dank verschuldigd aan iedereen die keer op keer bereid was om mijn vragen te beantwoorden.

Zoals eerder aangegeven in de inleiding wordt in dit onderzoek veelvuldig gebruik gemaakt van de termen watermerk, watermerktechniek en watermerksysteem. Met deze termen wordt, tenzij anders is aangegeven het volgende bedoeld. De term 'watermerk' verwijst naar de boodschap die in een signaal (computerbestand) is of wordt aangebracht.[5] Hierbij kan zowel worden gedacht aan verschillende type boodschappen zoals het verstrekken van informatie over de gebruiker of het bepalen van het gedrag (bv. kopiëren niet toestaan). De term 'watermerktechniek' wordt gebruikt voor de wijze waarop het watermerk wordt aangebracht in het gastobject inclusief daarbij gemaakte keuzes ten aanzien van de eigenschappen van het watermerk. Anders gezegd watermerktechnieken verwijzen naar methoden om boodschappen aan te brengen (embedden) en te detecteren. Het ver- en ontsleutelen van de boodschap wordt als deel van een watermerktechniek beschouwd.

2.2 Introductie digitale watermerken als techniek

Digitaal watermerken (hierna: watermerken) is kort gezegd een techniek die het mogelijk maakt informatie in een digitaal bestand te embedden. Sinds de opkomst in het begin van de jaren negentig staat deze techniek vooral in het teken van de handhaving van het auteursrecht. In deze paragraaf wordt het watermerk nader geïntroduceerd aan de hand van de geschiedenis van het watermerk (par. 2.2.1). Daarna wordt een classificatie van watermerken gegeven om duidelijk te maken welke soorten watermerken kunnen worden onderscheiden en welke plaats het onwaarneembare digitale watermerk inneemt (par. 2.2.2). Vervolgens wordt de techniek van watermerken nader onderzocht en gekeken naar de wijze waarop watermerken gebruik maken van de eigenschappen van digitale bestanden om de boodschap te verbergen en te beveiligen (par. 0). Ook is er aandacht voor de verschillende toepassingen van watermerken (par. 2.2.4). Om identificatie van de licentienemer mogelijk te maken is de wijze waarop de authenticatie van de licentienemer plaatsvindt van groot belang (par. 2.2.5). Omdat dat deel van het proces voor de techniek van watermerken nauwelijks interessant is, is daar in de watermerkliteratuur weinig aandacht voor.

2.2.1 Korte geschiedenis van watermerken

Watermerken worden van oudsher gevormd door herkenbare patronen in papier. De bekendste toepassing van watermerken is het gebruik daarvan in bankbiljetten.[6] Het is niet duidelijk waar het woord 'watermerk' zijn oorsprong vindt. In de periode tussen de 13^{e} en 18^{e} eeuw waren met name de Engelsen (watermark), Duitsers (wasserzeichen), Fransen (filigrane) en Nederlanders (papiermerken) actief met watermerken. De herkomst van de term wordt vaak toegeschreven aan de Engelsen omdat de Duitse schrijvers deze term pas aan het begin

[5] Een onzichtbaar watermerk heeft als hoofdeigenschap dat de karakteristieken van het signaal niet wijzigen. Een foto blijft dus een foto, waar wijzigingen in zijn aangebracht die voor de aanbrenger een bepaalde boodschap bevat.

[6] Zie voor een nader historisch perspectief o.m. het Bernstein project (www.bernstein.oeaw.ac.at/). Verder in de watermerkliteratuur ook Hartung & Kutter 1999; Moulin & Koetter 2005.

van de 19e eeuw gebruikten.[7] Behalve dat water noodzakelijk is bij het maken van papier is het niet duidelijk waarom deze techniek of het teken bekend is geworden als 'watermerk'.

Het oudste gewatermerkte papier is gevonden in Fabriano (Italië) en dateert van rondom het jaar 1282.[8] In die tijd was dit een bekende plaats voor de productie van papier. Het exacte doel van het aangebrachte watermerk is onzeker. Er worden dan ook verschillende functies aan toegeschreven, zoals decoratie van documenten tot het identificeren van de papiermolen of de maker van het watermerk. Watermerken werden in het begin gemaakt door dunne draden aan de papiermolen toe te voegen. Hierdoor was het papier op bepaalde plaatsen dunner en daardoor meer transparant.[9] Vanaf deze tijd verspreidde verschillende (water)merken en watermerktechnieken zich langzaam over Europa en later de Verenigde Staten.[10] In de loop der tijd worden de technieken verbeterd en wordt het mogelijk om door het gebruik van dunnere draden meer gedetailleerde ontwerpen te maken.

Met de introductie van nieuwe druktechnieken in de achttiende eeuw ontstonden er nog meer mogelijkheden om watermerken aan papier toe te voegen. Waar watermerken in de tussenliggende periode onder meer werden gebruikt als datumstempel voor de productie van papier kwamen watermerktechnieken in de achttiende eeuw ook op als middel om namaak te bestrijden.[11] Over de bewijswaarde van deze watermerken kan men grote twijfels hebben, mede gezien de gebrekkige kwaliteit van het watermerk. Watermerken waren in deze tijd niet altijd duidelijk of niet voorzien van een datum of locatie-aanduiding. Door het gebruik van watermerken in bankbiljetten kwam in de achttiende eeuw ook het vervalsen van watermerken op.[12] De schotse horlogemaker John Mathison is de bekendste vervalser van watermerken.[13] Hij had een methode ontdekt die het mogelijk maakte om de gewatermerkte bankbiljetten van de Darlingtonbank na te maken op een wijze die nauwelijks van echt te onderscheiden was. Na zijn arrestatie en bekentenis deed hij het voorstel om zijn methode prijs te geven op voorwaarde dat hij niet verder vervolgd zou worden. Die poging faalde. Hij werd in 1779 geëxecuteerd.[14]

---

[7] Zie o.m. Hunter 1978, p. 264; Cox e.a. 2008, p. 7. Zie voor watermerken uit de middeleeuwen onder meer het eerder genoemde Bernsteinproject.

[8] In de watermerkliteratuur worden verschillende data genoemd, zo noemen Katzenbeisser & Petitcolas 2000 (par. 5.2.1, p. 98) het jaar 1292 en Cox e.a. 2008 (par. 1.2, p. 6) het jaar 1282. De exacte datum is vooral onder historici onderwerp van discussie, zie o.m. Hunter 1978, p. 260; Harris 2010, hoofdstuk 5, referentie 19. Zie voor een verdere beschrijving van papierenwatermerkentechnieken o.m. Tschudin 2002; Harris 2010 en de website van de International Paper Historians: paperhistory.org.

[9] Zie ook Coelho e.a. 2009, die dezelfde techniek gebruiken voor 'Pulp-based computing. A Framework for Building Computers Out of Paper'.

[10] Het is niet duidelijk of deze technieken zich ook over de rest van de wereld hebben verspreid of dat watermerktechnieken zelfstandig zijn uitgevonden in andere delen van de wereld of vice versa.

[11] Zie o.m. Cox e.a. 2008, p. 6.

[12] Zie o.m. Hunter 1978, p. 264;

[13] In de zin dat hij in de watermerkliteratuur de meest genoemde vervalser is. Zie o.m. Hunter 1970, p. 281 (onder Mathieson); Cox 2008, p. 7.

[14] Gentleman's Magazine 1779, p. 374, meldt dat hij op woensdag 28 juli 1779 is geëxecuteerd. De wijze waarop het geëxecuteerd is blijft onduidelijk. Thornbury meldt in 1878 slechts dat 'he subsequently paid the full penalty of his crime'. Cox (2008, p. 7) die zich ook baseert op het eerder genoemde magazine meldt dat hij is

In deze periode werden enkele octrooien ten aanzien van het maken van papier of van watermerken vastgelegd.[15] Het gebruik van watermerken als juridisch bewijsmiddel neemt in deze periode toe. Zo leidde in 1887 het watermerk van de producent van het papier van twee brieven samen met ander bewijs uiteindelijk tot de vaststelling door de rechtbank dat twee brieven van een andere datum waren voorzien. De brieven droegen bij aan het bewijs dat de schoonzoon van de Franse president Grévy betrokken was bij het onterecht toekennen van de belangrijkste Franse onderscheiding (Légion d'honneur). Uiteindelijk zorgde dit incident in Frankrijk tot de vervolging van een afgevaardigde, het ontheffen van een politie-prefect uit zijn functie, de ondergang van een kabinet en uiteindelijk het ontslag van de president.[16]

Vanaf het begin van de jaren negentig van de twintigste eeuw neemt de aandacht voor het verbergen van informatie (steganografie) en het beschermen van de inhoud (cryptografie) vanuit de wetenschap toe. De belangrijkste reden daarvoor is de toenemende aandacht en zorg vanuit zowel de industrie als de politiek voor inbreuken op het auteursrecht dat op grote schaal en eenvoudig mogelijk is geworden door de opkomst van internet.[17] Watermerken moesten het nadeel van cryptografische systemen oplossen, dat er in bestond dat de content onbeschermd was nadat deze was ontsleuteld. Hierbij moet vooral worden gedacht aan toegangsbeveiliging. Watermerken bieden in die zin meer bescherming omdat het watermerk bij normaal gebruik niet wordt verwijderd en in tegenstelling tot cryptografie ook na de distributie bescherming biedt.[18]

In de literatuur wordt aangenomen dat de term ‘digital watermark’ in 1988 is geïntroduceerd door Komatsu and Tominaga. De techniek is echter al eerder beschreven in 1979 door Szepanski en platenmaatschappij EMI had al in 1988 een octrooi verkregen voor een methode voor ‘Encoded marking of a recording signal’.[19] Het eerste octrooi van wat wij nu aanduiden als een digitaal watermerk is op 29 april 1954 ingediend door Emil Frank Hembrooke van the Muzak Corporation New York bij het United States Patent Office voor ‘identification of sound and like signals’.[20] Het octrooischrift beschrijft allereerst het probleem: ‘The unauthorized recording and rebroadcasting of musical performances, for example, has been difficult to prevent because of the inability to detect positively whether the rebroadcast is an exact reproduction of the original or a different performance’. De daarvoor gegeven oplossing

opgehangen. Ook Hunter 1970 meldt dat hij is opgehangen. Ophanging lijkt gezien de straffen in die tijd de meest voor de hand liggende methode.

[15] Zie o.m. Hunter 1970, p. 131; Rückert, Hodeĉek & Wenger 2009, p. 22.

[16] Zie o.m. Katzenbeisser & Petitcolas 2000, p. 99 en voor meer voorbeelden in deze periode ook de The Americon stationer, februari 1888, p. 366. J. Weiner and K. Mirkes, Watermarking, no. 257 in Bibliographic Series, Appleton, Wisconsin: The Institute of Paper Chemistry, 1972.

[17] Zie o.m. Petitcolas, Anderson & Kuhn 1999, p. 1062; Delaigle 2000 (diss.), p. 2; Cox e.a. 2008, p. 8.

[18] Zie o.m. Cox e.a. 2008, p. 11.

[19] Komatsu & Tominaga 1998; zie Cox e.a. 2008, par. 1.2, p. 8. Szepanski 1979 (‘machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes’); Octrooi GB 2196167 (A), uitgevonden door L. Holt, B. G. Maufe, and A. Wiener.

[20] Emil Frank Hembrooke van the Muzak Corporation New York diende op 29 april 1954 een octrooi in bij het United States Patent Office voor ‘identification of sound and like signals’United States Patent, 3,004,104, 1961. Filed 29 april 1954, Ser. No. 426,465.

wordt als volgt omschreven: 'The present invention makes possible the positive identification of the origin of a musical presentation and thereby constitutes an effective means of preventing such piracy, i.e. it may be likened to a watermark in paper'. Muzak gebruikt dit systeem tot ongeveer 1984.[21]

De eerste artikelen over digitale watermerken verschijnen rond 1990 en hadden betrekking op digitale beelden.[22] Sindsdien is het een snel evoluerend onderzoeksgebied waarbij verschillende onderzoeksdomeinen, zoals statistiek, informatietheorie, codetheorie, speltheorie en signaalverwerking samenkomen.[23] Vanaf 1996 worden er verschillende bijeenkomsten georganiseerd rondom watermerken.[24] Ook vanuit de industrie en standaardisatieorganisaties nam de aandacht voor deze techniek toe.[25] Niet in de laatste plaats omdat sommige mediaondernemingen zouden hebben geweigerd om materiaal op DVD uit te geven zolang er geen aandacht zou worden besteed aan de bescherming van auteursrecht.[26] Vanuit het DVD-consortium wordt gevraagd naar mogelijkheden om het kopieergedrag te reguleren door middel van techniek (copymanagement).[27] In deze tijd is er ook veel aandacht voor het verbergen van auteursrechtinformatie en fingerprints in de vorm van een serie verborgen nummers met als doel om inbreukmakers op te kunnen sporen en te vervolgen.[28] Door middel van verschillende internationale onderzoeksprojecten stimuleert ook de Europese Commissie dit nieuwe onderzoeksdomein.[29] Watermerken als bewijsmiddel wordt veelal in het onderzoeksdomein van digitaal forensisch bewijs geplaatst.[30]

Tegelijkertijd komt vanuit het juridisch domein steeds meer aandacht voor de juridische bescherming van technische voorzieningen in verband met Digital Rights Management

[21] C. Walker. Personal communication, June 2000 ontleend aan Cox e.a. 2008, par. 1.2, p. 8. Zie voor meer historische voorbeelden over cryptografie, steganografie en watermerken o.m. Petitcolas, Anderson, Kuhn 1999, p. 1064; Cox e.a. 2008, p. 7.

[22] Tanaka, Nakamura & Matsui 1990; Caronni 1993; Tirkel e.a. 1993.

[23] Zo stijgt het aantal publicaties na Tanaka, Nakamura & Matsui in 1990 tot 103 publicatie in 1998 (Roch & Dugelay 1998; Katzenbeisser & Petitcolas 2000, p. 100). Cox e.a. 2008, par. 1.2, p. 9 laten een stijging zien van het aantal papers dat gepubliceerd is in *IEEE* ten aan zien van watermerken en steganografie van 0 in 1994 tot meer dan 900 in 2004. Zie voor de relatie van deze domeinen met watermerken o.m. Pérez-Pérez-Freire 2008, p. 7.

[24] De eerste academische bijkomst met aandacht voor digitale watermerken vond plaats tijdens 'The first Information Hiding Workshop (IHW)' bij het Isaac Newton Institute in Cambridge in England; Anderson 1996. Zie verder Petitcolas, Anderson & Kuhn 1999, p. 1062 ; Delaigle 2000 (diss.), p. 2; Cox 2008, p. 8.

[25] Zie o.m. DAVIC (Digital Audio Visual Council); DVD, TVAnytime, SDMI (Secure Digital Music Initiative), en MPEG (Moving Picture Experts Group) waren betrokken bij pogingen om tot een standaard te komen. Zie verder Petitcolas, Anderson & Kuhn 1999, p. 1062; Delaigle (diss.) 2000, p. 2.; Cox 2008, p. 8.

[26] Renaud 1996; Rupley 1996; Langelaar, Setywan & Lagendijk 2000, p. 20; Langelaar (diss. 2000), p. 1; Taylor, Johnson & Crawford 2007, p. 2-7. Guibault 2007, p. 15 signaleert hetzelfde voor major record labels. .

[27] Petitcolas, Anderson & Kuhn 1999, p. 1062; onder verwijzing naar Linnartz 1998 en Miller, Cox & Bloom 1998.

[28] Petitcolas, Anderson & Kuhn 1999, p. 1062.

[29] Zie o.m. ECRYPT(.eu.org) (European Network of Excellence for Cryptology). Zie verder Delaigle (diss.) 2000, p. 2. Maar ook nationaal, bijvoorbeeld in het kader van STW-projecten. Eind 2013 is in het CREST-project (Collusion RESistant Tracing) door TU Eindhoven, Civolution en Irdeto onderzoek verricht naar de veerkracht van digitale watermerken tegen collusion attacks (par.2.5) in het kader van traitor tracing.

[30] Zie o.m. Pérez-Freire 2008 (diss.), p. 1 en de verschillende congressen zoals het jaarlijkse SPIE-congres (Media Watermarking, Security, and Forensics).

(DRM) in de vorm van wetgeving, zowel in WIPO-verband (art. 11 en 12 WIPO Copyright Treaty, 1996) als in Europa (art. 6, 7 Richtlijn 2001/29/EG) en de Verenigde Staten (DCMA, 1998).[31]

Na de beginperiode, constateert Delaigle in zijn proefschrift in 2000 dat 'Fortunately, even if the ideal set of requirements will probably never be fulfilled by watermarking technologies, today's solutions are reaching a sufficient level to start to use watermarking commercially. (…) but in any case there is still quite some work to do.'[32] De integriteit van watermerkmethodologie en de beveiliging zijn in deze beginperiode aan stevige kritiek onderhevig.[33] In verschillende reacties daarop komt naar voren dat er (te) veel van deze techniek in dit jonge onderzoeksdomein werd verwacht en dat er in deze periode inderdaad nog geen methode bestond die in staat is om alle toekomstige aanvallen te weerstaan.[34] Niettemin sprak men de verwachting uit dat er nieuwe methoden zouden komen die steeds beter in staat zouden zijn om de genoemde problemen aan te pakken.[35] In deze periode werd er ook steeds kritischer gekeken naar de vraag of en zo ja welke data verborgen moeten worden en of dit niet eenvoudiger kan met andere technieken.[36] Watermerken blijven niettemin in de belangstelling staan. Ook het Amerikaanse Supreme Court ziet in de Grokster-zaak in 2005 digitaal watermerken nog als 'new technological devices that will help curb unlawful infringement.[37]

Het onderzoek naar digitale watermerken vindt tegenwoordig zowel binnen de industrie als in verschillende wetenschappelijke disciplines plaats.[38] In de watermerkliteratuur wordt watermerken inmiddels ook als voldoende volwassen beschouwd voor toepassing en commercieel gebruik.[39] Watermerken worden, naast de medische en reclamepraktijk, vooral toegepast in het kader van de handhaving van het auteursrecht. Zo gebruiken de meeste fotostockwebsites zichtbare watermerken om hun foto's te beschermen. Onwaarneembare watermerken worden onder meer gebruikt bij films die op Pay-TV of in een bioscoop worden

[31] Zie daarvoor uitgebreid het proefschrift van Koelman (2003). In 2005 komt de European Union's Data Protection Working Party met een Working document on data protection issues related to intellectual property rights gevolgd door reacties van EBLIDA (European Bureau of Library, Information and Documentation Associations); EuroISPA (European Internet Service Providers Association) en de DWWG (Digital Watermarking Working Group's).
[32] Delaigle 2000 (diss.), p. 3.
[33] Zie in het algemeen en los van de kritiek op specifieke onderdelen van watermerksystemen met name Herley (2000) in zijn artikel 'Why Watermarking is Nonsense'.
[34] Zie o.m. Craver, Wu & Liu 2001; Moulin 2003, Barni 2003a.
[35] De ontwikkeling van het creëren van aanvallen en tegenmaatregelen vormt een rode draad in dit domein.
[36] Zie o.m. Barni 2003b.
[37] MGM Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (27 juni 2005)
[38] De grootste ondernemingen: Aquamobile, Civolution, Datamark, Digimarc, Isan, Markany, MSI (Media Science International) en Verimatrix hebben zich verenigd in de Digital Watermarking Allicance(.org). Verschillende papers laten bovendien zien dat er veel auteurs na of naast een academische carrière werkzaam zijn in het bedrijfsleven. De disciplines waarin het onderzoek plaatsvindt verschilt, zo is Ingemar Cox tegenwoordig Professor of Communications aan het Department of Computer Science van het University College London en houdt Reginald Lagendijk een leerstoel Information and Communication Theory aan de TU Delft) bij de Multimedia Signal Processing Group.
[39] Zie o.m. Pérez-Pérez-Freire 2008 (diss.), p. 6.

aangeboden. Wanneer mensen deze films opnemen en op internet verspreiden heeft de rechthebbende de mogelijkheid om hotel- en bioscoopexploitanten aan te spreken op de genomen beveiligingsmaatregelen. Tegenwoordig worden ook e-boeken steeds vaker beveiligd met watermerken.[40]

2.2.2 Classificatie van watermerken

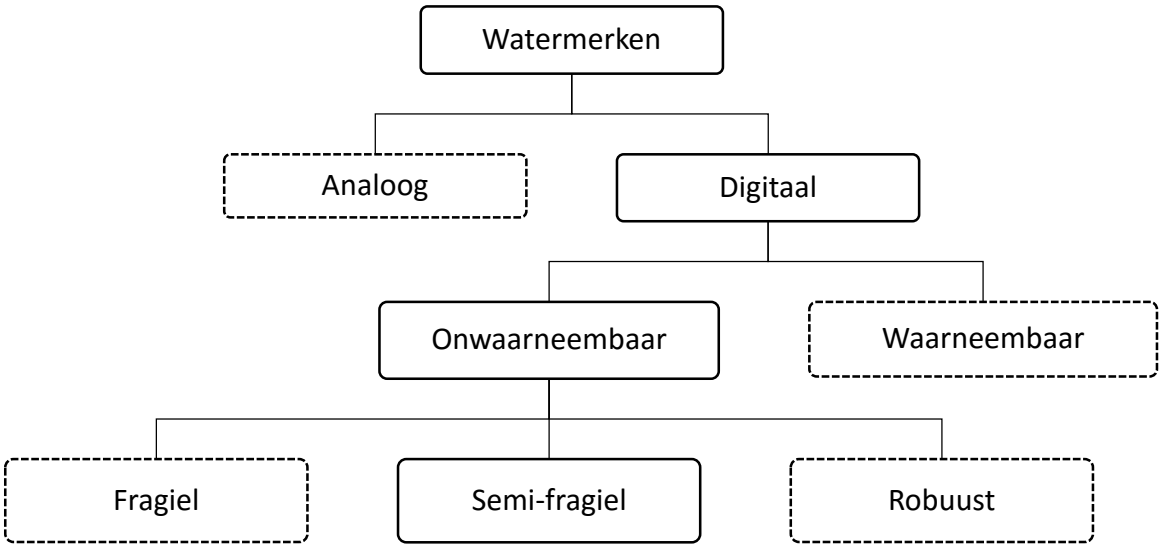
Watermerken worden in de literatuur op verschillende wijzen geclassificeerd, afhankelijk van het domein waarin het onderzoek plaatsvindt.[41] Wanneer watermerken centraal worden gesteld wordt ten eerste onderscheid gemaakt tussen analoge en digitale watermerken. Het onderscheid tussen beide ligt hier in het soort signaal. Digitaal watermerken kan in dat opzicht worden gezien als een communicatieproces met gebruik van een digitaal signaal. Alle andere processen kunnen dan als analoog worden gezien. Bij het gebruik van een watermerk in bijvoorbeeld Microsoft Office Word spelen beide processen een rol. Van analoge technieken is bijvoorbeeld gebruik gemaakt wanneer de tekst met een logo (watermerk) wordt geprint en het watermerk zichtbaar weergeeft. Bij het inbrengen van het watermerk wordt echter ook het digitale bestand veranderd en die verandering kan gekwalificeerd worden als een digitale techniek. Overigens wordt bij het printen ook een zogenoemd natuurlijk watermerk aan het papier toegevoegd doordat de printer zelf kleine (unieke) oneffenheden veroorzaakt tijdens het printproces. Deze natuurlijke watermerken maken het mogelijk dat de printer achterhaald kan worden waarmee het papier is geprint.[42] Ook dit proces kan als analoog worden getypeerd.

Bij digitale watermerken wordt vervolgens een onderscheid gemaakt tussen waarneembare en onwaarneembare watermerken. Ten aanzien van audio wordt veelal gesproken over onwaarneembare watermerken terwijl bij beelden (foto of video) zichtbare en onzichtbare de meest gangbare termen zijn. Waarneembare watermerken worden onder meer gebruikt ter bescherming van foto's die worden aangeboden op commerciële websites, zoals istock.[43] Het watermerk is daar duidelijk waarneembaar in het midden aangebracht zodat potentiele licentienemers de foto wel kunnen zien en zelfs kunnen kopiëren, maar zonder kwaliteitsverlies het watermerk lastig kunnen verwijderen. Zichtbare watermerken hebben als voordeel dat het direct zichtbaar is en daarmee duidelijk is dat het werk is beschermd. Bovendien kan het voor potentiële inbreukmakers een drempel opwerpen of deze zelfs afschrikken. Zij hebben echter als nadeel dat het de kwaliteit van het originele werk ook zichtbaar aantast. In vergelijking met onzichtbare watermerken zijn zij door de zichtbaarheid

[40] Bij e-boeken is het echter niet altijd duidelijk welke technieken hierbij worden ingezet en of deze technieken overeenkomen met de hier beschreven watermerkentechnieken. Bij e-boeken kan het ook voorkomen dat de rechthebbende woorden toegevoegd aan de tekst waardoor de tekst uniek is en daarmee traceerbaar wordt.
[41] Zie o.m. Katzenbeisser & Petitcolas 2000, hoofdstuk 6, p. 121. Zie ook par. 0 voor een indeling bij het verbergen van informatie (cryptologie).
[42] Daarnaast bestaan watermerken die aan printer worden toegevoegd, zie bijv. US patent 6,556,688 B1 voor Watermarking with random zero-mean patches for printer tracking (Epson).
[43] Zie verder o.m. Shutter Stock, iStockPhoto en Getty Images en de nationalebeeldbank (.nl).

ook eenvoudiger te verwijderen.[44] De gewenste toepassing zal daarbij mede afhangen van de aard van de organisatie. Organisaties, zoals musea die graag hun collecties willen tonen zonder kwaliteitsverlies kiezen dan eerder voor het gebruik van onzichtbare watermerken, zoals de Hermitage in Sint-Petersburg.[45]

Onwaarneembare watermerken kunnen verder (naar resistentie) worden onderscheiden in drie typen watermerken: fragiele (ontworpen om te degenereren bij de minste aanpassing aan de inhoud), robuuste (ontworpen om verschillende pogingen om het watermerk aan te tasten te overleven) en semi-fragiele watermerken, die de eigenschappen van de vorige twee combineren.



De keuze voor semi-fragiele watermerken zal later in paragraaf 2.4 nader worden toelicht, maar komt er in de kern op neer dat het voor watermerken met als doel de licentienemer te kunnen traceren niet wenselijk is dat het gastobject het watermerk verliest, maar ook niet dat het te allen tijde robuust is. Een semi-fragiel watermerk combineert beide eigenschappen en moet ervoor zorgen dat het aantasten van het watermerk ook leidt tot kwaliteitsverlies van bijvoorbeeld de film waarin het watermerk is aangebracht. De eerder benoemde trade-off tussen de verschillende eigenschappen speelt hierbij een belangrijke rol.[46] Naast deze indeling wordt er ten aanzien van digitaal watermerken ook onderscheid gemaakt tussen de verschillende soorten embedding en detectie die mogelijk zijn.[47]

[44] Zie voor zichtbare watermerken en de bescherming van auteursrechten uitgebreid Delaigle 2000 (diss.)
[45] Zie ook de waarschuwing op hun website: 'Images on this web site have been invisibly watermarked.' hermitagemuseum.org/html_En/00/hm0_7.html. Zie ook Brunopress.nl (Vzr. Rb. Amsterdam 16 oktober 2008, ECLI:NL:RBAMS:2008:BG0972, Mf 2008-11/12, nr. 39, p. 456 m.nt. AlberdingkThijm (Bruno Press/IMT).
[46] Zie verder paragraaf 2.4.
[47] Een presentatie van een dergelijke indeling is echter pas zinvol bij een keuze voor een specifiek systeem en wordt dan ook verder niet worden besproken Zie daarvoor o.m. Cox e.a. 2008.

2.2.3 Digitaal watermerken als techniek

Bij het ontwikkelen van onwaarneembare digitale watermerken wordt gebruik gemaakt van verschillende technieken en principes uit de cryptografie en steganografie. Cryptografie of geheimschrift ziet kort gezegd op het afschermen van de inhoud van boodschappen door het versleutelen van de informatie.[48] Doordat de sleutel bekend is bij de ontvangende partij kan de versleutelde boodschap door de ontvanger worden ontsleuteld en gelezen. Steganografie maakt een onderdeel uit van de cryptografie maar richt zich op het verbergen van boodschappen. Als belangrijkste verschil tussen enerzijds cryptografie en steganografie en anderzijds watermerken wordt vaak de robuustheid genoemd die het watermerk moet beschermen tegen aanpassingen van het watermerk.[49] Ten aanzien van het verborgen karakter van watermerken wordt deze techniek gezien als een bijzondere vorm van steganografie.[50]

Een principe uit de cryptografie dat eveneens een belangrijke rol speelt bij watermerken is de zogeheten wet van Kerckhoffs. Hij stelde dat men er niet vanuit mag gaan dat de methode geheim blijft en het geen probleem mag opleveren als de methode bekend wordt. [51] Anders gezegd, het succes van het systeem moet niet van afhangen van de geheimhouding van de methode, maar slechts van de geheimhouding van de sleutel zelf.[52] Strikt genomen is het niet noodzakelijk om de methode of het systeem geheim te houden. Voor het uitlezen van de boodschap is het wel noodzakelijk om de sleutel in handen te hebben. De betrouwbaarheid van een systeem kan eventueel nog worden nagebootst, maar een compleet geheim systeem maakt de presentatie en controle op het bewijs wel veel moeilijker. Wanneer wij ervan uitgaan dat het bestaan van het watermerk bekend is, bijvoorbeeld doordat men hiervoor gewaarschuwd is, dan zal het watermerk in overeenstemming met de wet van Kerckhoffs voldoende robuust moeten zijn om te voorkomen dat het watermerk wordt verwijderd of zodanig wordt aangetast dat het niet meer kan worden gedetecteerd.

Voor het verbergen van extra informatie in digitale objecten wordt bij watermerken gebruik gemaakt van verschillende technieken. Watermerktechnieken voor het verbergen van extra informatie in afbeeldingen, audio en video, maken in de basis allemaal gebruik van het idee dat een digitaal bestand bestaat uit een binaire code van nullen en enen. Hierdoor is het mogelijk om met behulp van verschillende wiskundige modellen berekeningen uit te voeren

[48] Zie o.m. Van den Eshof 2002; Cox 2008, p. 9.
[49] Zie o.m. Katzenbeisser & Petitcolas 2000, p. 2. Zie uitgebreid voor de overeenkomsten en verschillen: Petitcolas, Anderson, Kuhn 1999; Katzenbeisser & Petitcolas 2000; Cox e.a. 2008, hoofdstuk 12 en 13.
[50] Zie o.m Van den Eshof 2002 e.a., p. 98; Koelman 2003 (diss.) p. 30. Petitcolas, Anderson, Kuhn 1999, p. 1063; Katzenbeisser & Petitcolas (2000, p. 1) zien het als een aparte groep van technieken naast Covert channels, Anonymity en Steganography.
[51] 'Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi'. Kerckhoffs 1883, p. 12. Shannon (1949, p. 662) nam als vertrekpunt 'the enemy knows the system' ('Shannon's maxim'). 'To make the problem mathematically tractable we shall assume that the enemy knows the system being used. That is, he knows the family of transformations Ti, and the probabilities of choosing various keys.'.
[52] In het algemeen wordt ervan meerdere cryptografische sleutels gebruik gemaakt om te voorkomen dat anderen het watermerk kunnen manipuleren of verwijderen. Met de sleutel kunnen immers ook de embeddingsstrategie en de locaties van de watermerken bekend worden.

en op verschillende wijzen boodschappen in deze bestanden te verbergen. De mate waarin en wijze waarop een boodschap kan worden verborgen, hangt daarmee samen met de beschikbare binaire code en de gebruikte techniek. Om de verschillende processen te optimaliseren zijn er verschillende technieken ontwikkeld voor verschillende soorten (afbeeldingen, audio, video,) en typen (MP3, MPEG4, JEPG) bestanden. Bij het verbergen van een boodschap (watermerk) speelt tevens de kwaliteit van de content een belangrijke rol. De kwaliteit van het object heeft een directe invloed op de hoeveelheid informatie die kan worden verstopt en op de waarneembaarheid van het watermerk. Immers, hoe hoger de kwaliteit van bijvoorbeeld een foto, hoe meer bits er worden gebruikt en hoe meer ruimte er is om een boodschap te verbergen zonder dat er sprake is van waarneembaar kwaliteitsverlies. Het verbergen van informatie is om die reden eenvoudiger in afbeeldingen, audio, en video dan in tekstbestanden. Tekstbestanden bevatten veel minder binaire code en daardoor ook minder 'ruimte' om informatie in te stoppen.

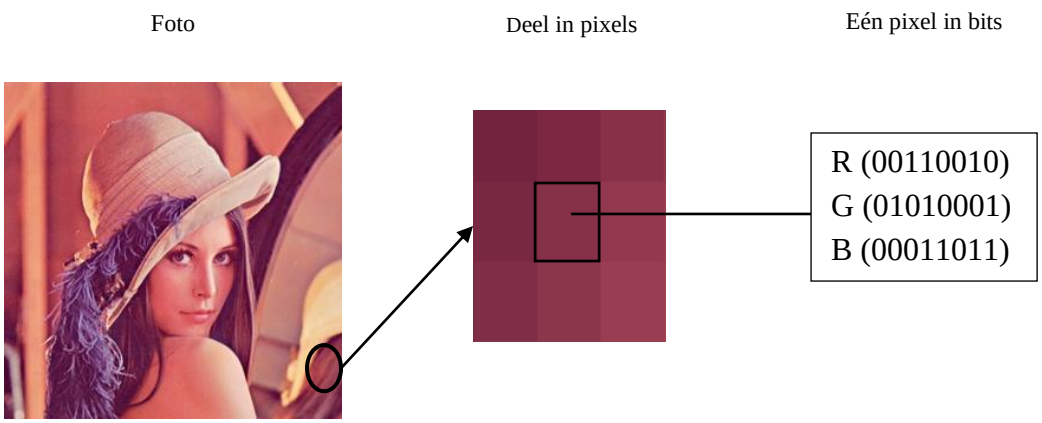
De eenvoudigste manier om informatie in een signaal te verstoppen zijn technieken die gebaseerd zijn op het vervangen van bepaalde bits (bitplane), zoals de Least Significant Bit modification of subsitution (LSB).[53] Deze technieken veranderen de eigenschappen van een bestand, bijvoorbeeld door de kleur van één pixel in een afbeelding te veranderen. Doordat de ontvanger toegang heeft tot de sleutel kan alleen hij zien waar de verschillen zich bevinden en welke boodschap die verschillen dragen.

Aan de hand van deze eenvoudige techniek (LSB) is goed duidelijk te maken hoe het verbergen van informatie werkt. In beginsel werkt deze toepassing hetzelfde bij afbeeldingen, audio en video. In alle gevallen geldt hoe hoger de kwaliteit van het bestand, hoe eenvoudiger het is om informatie te verbergen. Een digitale foto is in beginsel niets meer dan een computerbestand en bestaat uiteindelijk uit een serie van nullen en enen. Wanneer wij naar een digitale foto kijken dan is deze opgebouwd uit veelal miljoenen pixels.[54] De kleur van een pixel wordt in beginsel gevormd door drie hoofdkleuren (rood, groen en blauw) die door hun onderlinge verhouding verschillende mengkleuren mogelijk maken.[55] Iedere kleur en daarmee iedere pixel is uiteindelijk weer opgebouwd uit een binaire code (nullen en enen). Deze code kan door het gebruik van verschillende technieken op verschillende wijzen worden weergegeven.

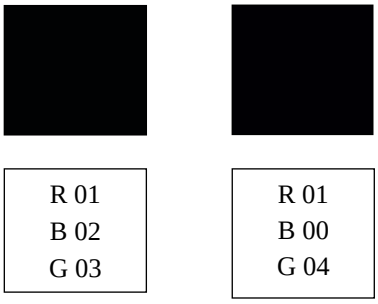
[53] Katzenbeisser & Petitcolas 2000, hoofdstuk 3, p. 43.

[54] Een camera van 5.0 megapixels kan gebruik maken van vijf miljoen verschillende pixels. Dit maakt het mogelijk om geleidelijk een kleurovergang te maken en dus scherpere foto's. In de praktijk wordt de pixelsdichtheid weergegeven in het aantal pixels per inch (DPI), dat wil zeggen het aantal pixels dat binnen hetzelfde gebied wordt weergegeven. Hoe meer, hoe scherper de foto.

[55] Afbeeldingen kunnen in verschillende formaten voorkomen zoals JPEG, BMP, PNG of GIF. Niettemin bestaat elke afbeelding uit pixels die afhankelijk van de gebruikte kleurcodering van een bepaalde code worden voorzien. In dit voorbeeld wordt gebruik gemaakt van een binair-stelsel met een kleurdiepte van 24 bits en de kleurcodering RGB of RGB-waardes (Rood-Groen-Blauw). Dat betekent 8 bits voor rood, 8 voor groen en 8 voor blauw. Bij audio kan men de pixel vervangen voor een frequentie. Deze kleuren worden vaak uitgedrukt in 8 bits en kan variëren tussen 00000000 en 11111111 of tussen 0 en 255 omdat iedere kleur (R,G,B) in 256 tinten kan voorkomen. Iedere pixel kan dan uit ± 16,7 miljoen kleuren (256*256*256) bestaan.



Doordat een foto van bijvoorbeeld Lena (links) is opgebouwd uit verschillende pixels (midden) met ieder een eigen kleur(-code) (rechts), is het op het eerste gezicht niet waarneembaar dat één pixel een andere kleur heeft.[56] Om duidelijk te maken dat een kleine wijziging lastig waarneembaar is zijn hieronder twee pixels 'zwart' opgenomen.[57]



Een verandering is waarneembaar in uniform grote vlakken, maar niet in gebieden met veel detail of patronen. De verandering is bijvoorbeeld bij de hierboven afgebeelde Lena lastig waarneembaar in haar donkere haar of paarse pluim. Door de erg kleine wijzigingen is de LSB techniek onzichtbaar. Ze is echter ook niet erg robuust omdat iedere verandering in de afbeelding ook de boodschap kan veranderen of verwijderen, bijvoorbeeld doordat iemand de afbeelding comprimeert.

Bij audio kan ook gebruik worden gemaakt van methoden die willekeurig geluiden toevoegen en verspreiden over het audio-bestand (Spread Spectrum) of het toevoegen van extra geluiden aan de echo. Bij audio, video en afbeeldingen wordt ook wel gebruikt gemaakt van Discrete Cosine Transform (DCT) die het mogelijk maakt om in elk beeldfragment een kleine verandering aan te brengen.[58] Het verbergen van informatie in video's is enerzijds

[56] Lena of Lenna is de meest gebruikte afbeelding in de literatuur over image processing algorithms. De foto is afkomstig uit de Playboy en riep naast auteursrechtelijke vragen ook diverse vragen op over overheersing van mannen in de computerwetenschappen. Zie uitgebreid met verwijzingen in de literatuur: http://en.wikipedia.org/wiki/Lenna.

[57] Visueel is dit ook eenvoudig in Microsoft word na te maken door en vak te vullen (emmertje ;) en de kleuren aan te passen. Wanneer één van de drie kanalen met een cijfer wordt verhoogd of verlaagd dan is het verschil nauwelijks waarneembaar. Vanzelfsprekend verandert er hierdoor ook iets in de binaire code.

[58] Voor audio, beelden en video gaat men meestal naar een transformatiedomein.

vergelijkbaar met de wijze waarop dat ook met afbeeldingen gebeurt en kan dan onder meer plaatsvinden in de frames zelf, anderzijds kan de informatie ook verborgen worden in de manier waarop de frames elkaar opvolgen. Het voordeel van deze presentaties (anders dan bij foto's) is dat je gemakkelijker kan sturen op de trade-off zichtbaarheid/robuustheid en dat de eigenschappen het daar ook toelaten om deze te optimaliseren. In tekstbestanden, zoals e-boeken worden gegevens vaak verstopt in lege ruimten zoals spaties, enter of tabs.[59]

2.2.4 Toepassingen van watermerktechnieken

Watermerken worden voor verschillende doeleinden gebruikt, zoals het monitoren van bijvoorbeeld verkeer op internet of televisie (Broadcast Monitoring), voor het authenticeren, indexeren en verbergen van data of voor medische toepassingen bijvoorbeeld in het kader van patiëntveiligheid.[60] Watermerken kunnen ook in een poster worden verwerkt zodat de code ook na de print nog kan worden uitgelezen.[61] Zoals bij veel ICT-systemen geldt ook bij watermerksystemen dat er een wisselwerking of zelfs trade-off plaatsvindt tussen de functionele eisen en de in te zetten eigenschappen van de techniek.[62] De eerste vraag die van belang is bij het inzetten van watermerken is de vraag naar het doel of de toepassing van het systeem. De meeste toepassingen dienen, evenals het object in dit onderzoek, de bescherming van het auteursrecht en worden in de literatuur benoemd aan de hand van vier gebruikersdoelen.[63]

Ten eerste toepassingen die zien op authenticatie van content.[64] Voor authenticatie van content wordt veelal gebruik gemaakt van zogenoemde fragiele watermerken waarbij de robuustheid beperkt is. Deze watermerken zijn ontworpen om te degenereren bij de minste aanpassing aan de inhoud. Om watermerken gewone gebruikshandelingen te laten overleven wordt gebruik gemaakt van zogenoemde semi-fragiele watermerken die wel in staat zijn om bijvoorbeeld compressie te overleven.[65]

Ten tweede toepassingen die kunnen worden omschreven als regulering van content. De bekendste vorm daarvan is de kopieerbeveiliging.[66] Op basis van de informatie die het watermerk bevat kunnen, ten aanzien van de content, bepaalde handelingen worden verboden

[59] Bij e-boeken maakt men daarnaast vaak gebruik van zichtbare watermerken in de vorm van codes die uiteindelijk verwijs naar de licentienemer. Zie o.m. Bill Rosenblatt in zijn blogpost over Harry Potter: http://copyrightandtechnology.com/2012/04/08/the-harry-potter-watermarking-experiment/

[60] Zie voor andere toepassingen ook TNO 2010, p. 32.

[61] Zo maakt het kindermerk Fred & Ed gebruik van digitale watermerktechnologie die het mogelijk maakt een verpakking te scannen met een smartphone of tablet waarna het tot leven komt in een directe link naar een animatie. http://www.marketingonline.nl/nieuws/bericht/freded-pratende-verpakkingen/

[62] Uiteindelijk vindt er zowel een wisselwerking plaats tussen de functionele eisen zelf (bv. Robuustheid en waarneembaarheid) als tussen de doelen en gekozen techniek.

[63] Zie daarvoor o.m., Katzenbeisser & Petitcolas 2000, p. 103; Langelaar, Setywan & Lagendijk 2000, p. 20; Van den Eshof 2002, p. 98; Cox e.a. 2008, p. 15.

[64] Zie o.m. Katzenbeisser & Petitcolas 2000, p. 105 (Watermarking for Image Authentication); Langelaar, Setywan & Lagendijk 2000, p. 21 (Data Authentication); Cox e.a. 2008, p. 25 (Content Authentication).

[65] Zie ook voor meer voorbeelden Cox e.a. 2008, hoofdstuk 11 (p. 375).

[66] Katzenbeisser & Petitcolas 2000, p. 104 (Watermarking for Copy Protection); Copy protection (Langelaar, Setywan & Lagendijk 2000, p. 20; Copycontrol (Cox e.a. 2008, par. 2.1.6, p. 27).

of juist worden toestaan. Denk hierbij aan het wel of niet kunnen kopiëren of aan handelingen met codes als 'copy once'.

Ten derde eerste identificatie van de maker.[67] Deze toepassing ziet op het gebruik van watermerken om informatie, zoals de naam van de rechthebbende en het jaar van publicatie, in het gastobject aan te brengen. Deze toepassing heeft als doel om aan te tonen wie de maker is en om te voorkomen dat een ander het werk ten onrechte kan opeisen als zijn werk. Het watermerk zelf dient voor deze toepassing in ieder geval robuust te zijn. Daarnaast zal er bij het ontwerp en het gebruik van het watermerk rekening gehouden moeten worden met het toevoegen van watermerken door anderen. Hierdoor kan er een zogenoemde deadlock ontstaan wanneer meerdere partijen, op basis van ieder hun eigen watermerk, het makerschap claimen.[68]

Tot slot toepassingen die in dit onderzoek centraal staan en kunnen worden omschreven als (Traitor) Tracing.[69] Deze toepassing wordt ook wel aangeduid als 'fingerprinting' en heeft als doel objecten te identificeren en informatie te geven over de rechthebbende en zijn ontvanger, bijvoorbeeld een licentienemer.[70] Het watermerk bestaat dan veelal uit een unieke code die verwijst naar de maker of ontvanger van het gewatermerkte bestand.[71] Voor deze toepassing van watermerken is een hoge mate van robuustheid vereist tegen in ieder geval veel voorkomende dataverwerkingsprocessen en malafide aanvallen.[72] Bij deze toepassing wordt ook vaak gebruik gemaakt van watermerken waarbij het idee is dat het watermerk of voldoende robuust is om de boodschap uit te kunnen lezen of bij een malafide aanval op het watermerk de kwaliteit van de content zo laag wordt dat het niet langer interessant is om de content te gebruiken. Een bekend voorbeeld is het inzetten van watermerken om achteraf te kunnen beoordelen wie bijvoorbeeld politieke documenten lekt, zoals de zaak van Paul Tang van de PvdA die in 2009 de miljoenennota voor het embargo al naar de media had gelekt.[73]

---

[67] Er worden in de literatuur verschillende benamingen en categorieën voor deze doelen gebruikt. De omschreven doelen komen echter nagenoeg overeen. Zo benoemen Katzenbeisser & Petitcolas (2000, p. 104) en Langelaar, Setywan & Lagendijk (2000, p. 20) deze categorie als Copyright Protection; als Copyright Protection en Cox e.a. (2008, p. 19) het als Owner Identification en Proof of Ownership.

[68] Zie daarover o.m. Kwok 2003, p. 100.

[69] Fingerprinting for Traitor Tracking of Labelling (Katzenbeisser & Petitcolas 2000, p. 100, 104); Fingerprinting (Langelaar, Setywan & Lagendijk 2000, p. 20; Cox e.a. (2008, p. 24) gebruiken de term Transaction Tracking omdat, 'the person responsible for misuse of a Work is sometimes referred to as a traitor, whereas a person who receives the Work from a traitor is a pirate. As this distinction is not meaningful when discussing other applications where piracy is an issue, we do not use this terminology'. Er wordt ook wel gewezen op een forensisch watermerk (TNO 2010, p. 34).

[70] De term fingerprinting wordt in de signaalverwerkingsliteratuur ook gebruikt wordt voor technieken die het enkel mogelijk maken het signaal te identificeren en bijvoorbeeld indexatie mogelijk te maken. Zie o.m. Cano e.a 2005, p. 234.

[71] Zie uitgebreid o.m. hoofdstuk 8 Katzenbeisser & Petitcolas 2000, p. 175; Cox e.a. 2008, p. 23. Zie met betrekking tot de code ook de capaciteit van het watermerk (par. 2.4.4).

[72] Bij het versturen van een bestand van bijvoorbeeld een laptop naar het internet ondergaat het bestaande een aantal verwerkingen waardoor er kleine verschillen kunnen ontstaan. Ook is het denkbaar dat in bijvoorbeeld een afbeelding wordt gesneden. Daar tegenover staande aanvallen die met opzet worden uitgevoerd om het watermerk aan te tasten. Het watermerk moet voldoende robuust zijn om die veel voorkomende processen en aanvallen te kunnen weerstaan.

[73] RTLnieuws had in 2009 het document op de website gezet waarna de website GeenStijl met behulp van Photoshop de watermerken zichtbaar maakte. Ook Margaret Thatcher zou in 1981 al gebruik hebben gemaakt van technieken deze problemen onder minister te voorkomen. Zie o.m. Anderson 1996, p. 39; Langelaar 2000, p. 7 en Cox e.a. 2008, p. 5.

Watermerken met een traceerdoel worden onderscheiden in watermerken die voorzien zijn van een individuele boodschap zoals een naam of identificatienummer en boodschappen die bedoeld zijn voor generiek gebruik, waarin een groep identificeerbaar is maar niet de groepsleden op individueel niveau. Bij de eerste categorie kan gedacht worden aan een selecte groep filmrecensenten die per persoon een gewatermerkte film mee krijgen om te recenseren. In de twee categorie kan gedacht worden aan bijvoorbeeld gewatermerkte films in een bioscoop. De groep bioscoopbezoekers is mogelijk als groep te identificeren maar een individuele bezoeker kan niet geïdentificeerd worden. Dergelijke watermerken maken het mogelijk om bijvoorbeeld de bioscoop te identificeren en aan te spreken op een gebrekkige beveiliging.[74] Deze toepassing wordt ook in de filmindustrie gebruikt om de fases tussen ontwikkeling en eindgebruiker goed te bewaken. Op deze wijze kan worden bepaald in welke fase een film is uitgelekt, waardoor de beveiliging kan worden verbeterd of de kring waarbinnen gezocht moet worden kan worden verkleind. Hierbij kan gedacht worden aan mensen die betrokken zijn bij de productie maar ook aan recensenten of juryleden die voortijdig de beschikking hebben gekregen over bepaalde content. De boodschap die het watermerk draagt is afhankelijk van de situatie waarin deze wordt ingezet. Bij bioscopen zal de boodschap veelal bestaan uit tijden en/of locaties en bij pay-tv in hotels zal het eerder gaan om het opnemen van een datum, tijdstip en kamernummer. In dit laatste geval zal het veel eenvoudiger zijn om een individu aan te spreken op het schenden van het auteursrecht, in de regel omdat hij de licentievoorwaarde (gij zult niet kopiëren en verspreiden) overtreedt.[75]

De bekendste rechtszaak waarin deze toepassing een belangrijke rol speelde was de zaak van de acteur Carmine Caridi. Technicolor had in 2004 alle films die werden meegegeven aan alle 5803 leden van de Academy die mochten stemmen over de oscaruitreikingen voorzien van individuele watermerken. De ontvangers tekenden voor de kennisgeving dat het hen niet was toegestaan de ‘screeners’ te kopiëren en te verspreiden omdat een dergelijk feit een overtreding was van federale wetgeving.[76] Toen na de uitgifte bleek dat er twee films op internet waren verschenen werd duidelijk dat deze films waren uitgegeven aan de acteur Carmine Caridi. Na hierop te zijn aangesproken door de FBI gaf hij toe dat hij kopieën van deze films aan zijn vriend Russell Sprague had gegeven.[77] Hoewel Caridi aangaf niets te hebben geweten van de intenties van zijn vriend was hij niet langer welkom op de Academy en werd veroordeeld tot betaling van de maximale wettelijk toegestane schadevergoeding

[74] Dit leidde bijvoorbeeld in 2005 in Amerikaanse bioscopen tot personeel dat met nachtkijkers actief op zoek ging naar mensen die met een camera opname van de film probeerden te maken. In Duitsland leidde dit tot de verplichting bezoekers hiervoor te waarschuwen. http://www.spiegel.de/kultur/kino/jagd-auf-raubkopierer-kinozuschauer-muessen-ueber-nachtsichtgeraete-informiert-werden-a-652685.html

[75] Op grond van de auteurswet is het, behoudens de beperkingen bij wet gesteld, enkel de rechthebbende die zijn werk mag openbaar maken en verveelvoudigen. In de praktijk zal een gebruiker bijvoorbeeld wel toestemming krijgen om de content te bekijken, maar niet om deze verder op internet te verspreiden. Zie verder 2.2.5 en par. 3.4.

[76] ‘I agree not to allow the screeners to circulate outside my residence or office. I agree not to allow them to be reproduced in any fashion, and not to sell them or to give them away at any time.’

[77] Het ging in deze zaak om de films: The Last Samurai en Mystic River die Sparque van VHS had gedigitaliseerd. Zie verder http://www.imdb.com/name/nm0137142/news?year=2004.

(statutory damages) van $150.000 per titel aan Warner Bros.[78] Uiteindelijk heeft hij op basis van het watermerk het verspreiden van de films toegegeven. Tot een veroordeling op basis van het watermerk is het nooit gekomen.

In dit onderzoek staat met name deze laatste toepassing centraal waarbij het technisch mogelijk is om de naam van of gegevens die betrekking hebben op de licentienemer als boodschap in een gastobject op te nemen om later identificatie mogelijk te maken.[79] Om dat mogelijk te maken moet het watermerk enerzijds onwaarneembaar zijn zodat het kijk- en luisterplezier niet wordt verstoord en anderzijds ook in staat zijn om manipulaties te overleven.

2.2.5 Authenticatie van de licentienemer

Om de effectiviteit van het watermerk als bewijsmiddel te kunnen bepalen is het zowel van belang om vast te stellen dat de gegevens die in het watermerk zijn aangebracht correct zijn als dat de gebruikte watermerktechnieken om deze gegevens in het watermerk aan te brengen integer zijn. In de watermerkliteratuur richt men zich volledig op het watermerk als techniek en worden de gegevens die in het watermerk worden opgenomen als een vaststaand feit beschouwd waardoor er vanuit de watermerkliteratuur geen aandacht is voor de vraag of deze gegevens correct zijn. Voor het watermerk als bewijsmiddel is zowel de betrouwbaarheid van de gegevens die in het watermerk worden gestopt als de betrouwbaarheid van het watermerk als techniek relevant. In een hoofdstuk over de technische beschrijving van watermerken is dit dan ook een - niet onbelangrijk - intermezzo.

In de juridische literatuur is de authenticatie van personen uitgebreid behandeld bij de invoering van de gekwalificeerde elektronische handtekening en door de Nederlandse wetgever in de Memorie van Toelichting bij bijvoorbeeld Wet elektronisch bestuurlijk verkeer (hierna: WEBV).[80] Authenticatie van personen ziet enerzijds op de vraag of een bepaald

[78] United States District Court, Central District of California, 18 november 2004, 346 F. Supp. 2d 1068. (2004 WL 2755842) inzake Warner Bros. v. Carmine Caridi et al. Caridi werd veroordeeld bij verstek (Default Judgment) en Spraque sloot op 23 maart 2004 een plea agreement with the United States Attorney's Office. Sprague gaf uiteindelijk toe ongeveer 200 illegale kopieën te hebben gemaakt. Voordat hij veroordeeld kon worden tot drie jaar gevangenisstraf overleed hij in zijn cel aan een hartaanval. ‘Man in Piracy Case Found Dead’, Los Angeles Times, March 1, 2005 http://articles.latimes.com/2005/mar/01/business/fi-sprague1

[79] Hoewel dit onderzoek zich beperkt tot digitale bestanden is het ook mogelijk om na verwerking van bijvoorbeeld een poster de print te onderzoeken op watermerken, bijvoorbeeld nadat een afbeelding in een catalogus is verwerkt.

[80] Zie ook o.m. Voulon (diss.), p. 251; Van Stekelenburg 2009 (diss.), p. 26 en de verwijzingen aldaar. Zie voor de omzetting van de richtlijn 1999/93/EG (elektronische handtekening) naar zowel Nederlands als Belgisch recht: o.m. Lodder, Dumortier en Bol 2005; MvT bij de Wet elektronisch bestuurlijk verkeer, Kst II 2001/02, 28 483, nr. 3. Deze richtlijn (1999/93/EG) wordt op 1 juli 2016 vervangen door de inmiddels in werking getreden Verordening (EU) nr. 910/2014 van het Europees Parkement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Zie o.m. Voulon 2013.

persoon ook daadwerkelijk degene is voor wie hij zich uitgeeft en anderzijds of een gegeven inderdaad van hem afkomstig is.[81]

De Memorie van Toelichting bij de WEBV onderscheidt in theorie drie maten van betrouwbaarheid en vertrouwelijkheid (hierna: betrouwbaarheid).[82] Ten eerste de maximale betrouwbaarheid. Daarvan is sprake indien de beveiliging geheel conform de maximaal (technische) mogelijkheden plaatsvindt. Ten tweede een voldoende mate van betrouwbaarheid waarvan sprake is wanneer de veiligheid even groot is vergeleken met de situatie dat er uitsluitend van conventioneel verkeer gebruik zou worden gemaakt. En ten derde de zogenoemde pro-forma betrouwbaarheid waarvan sprake is indien de beveiliging slechts één stap verwijderd is van het bieden van geen enkele beveiliging. In de Memorie van Toelichting wordt tevens terecht vermeld dat absolute betrouwbaarheid niet bestaat en wat maximaal haalbaar is, afhankelijk is van de stand van de techniek en de (financiële) inspanningen die men ervoor over heeft.[83] In technische zin zijn er voldoende middelen die voldoende mate van zekerheid geven.[84] Rechthebbenden sluiten in de praktijk overeenkomsten met de aanbieders van content waarin zij afspraken maken over de mate waarin de content beveiligd moet worden voordat deze aangeboden mag worden. Hoewel deze afspraken geheim worden gehouden door middel van contractuele bepalingen mag worden aangenomen dat bij het opstellen van deze eisen zowel rekening wordt gehouden met de stand van de techniek als de gedachte dat de eindgebruiker (consument) bereid is de gestelde mate van beveiliging te aanvaarden.[85] De mate van betrouwbaarheid hangt daarmee samen met verschillende factoren die in een rapportage een plaats horen te krijgen om de betrouwbaarheid van authenticatie van personen te verantwoorden.

Het zal duidelijk zijn dat wanneer iemand onder een andere naam een licentie afsluit en als zodanig in het watermerk wordt opgenomen, ook een technisch volledig betrouwbaar watermerk uiteindelijk niet de daadwerkelijke licentienemer aanwijst. Vanuit het perspectief van de rechthebbende is dat onwenselijk omdat hij dan niet in staat is om de juiste persoon civiel- dan wel strafrechtelijk aan (te laten) spreken. Bijvoorbeeld omdat de licentienemer niet bestaat zoals bij namen als ‘Pietje Puk’, ‘Pak me dan’ of ‘Anomaly’. Vanuit het perspectief van de gedaagde of verdachte is dit onwenselijk omdat hij dan onterecht wordt aangesproken.

Een van de meer betrouwbare inlogprocedures die een rechthebbende in de praktijk kan hanteren is het gebruik van een methode die voldoet aan de eisen van de gekwalificeerde

[81] Zie o.m. Van Stekelenburg 2009 (diss.), p. 28.
[82] MvT bij de Wet elektronisch bestuurlijk verkeer, Kst II 2001/02, 28 483, nr. 3, p. 17.
[83] Idem.
[84] Zie voor een bespreking daarvan o.m. Van Stekelenburg 2009 (diss.), p. 31.
[85] Dat de (technische) wens van rechthebbende niet leidend is, is ook gebleken uit de inzet van kopieer-beveiliging die uiteindelijk heeft gefaald omdat de eindgebruiker de effecten van de inzet daarvan niet accepteerden. Zie par. 3.2.1.

elektronische handtekening.[86] De toepassing van een dergelijke methode levert de rechthebbende ook juridisch een voordeel op in de vorm van een wettelijk bewijsvermoeden.[87] In de praktijk zijn deze systemen complex en weinig populair bij webwinkels die klanten graag een eenvoudige toegang geven tot hun producten.[88]

De mate van zekerheid zal mede worden bepaald door de eisen die rechthebbenden stellen aan het niveau, namelijk die mate van zekerheid die bij aanbieders van content gevraagd wordt en die gebruikers bereid zijn te aanvaarden.[89] De betrouwbaarheid van de gegevens die worden verkregen is onder meer afhankelijk van de procedure die de aanbieder van content hanteert. Rechthebbenden en aanbieders van content maken contractueel afspraken over de beveiliging van de content. Complexe systemen zullen ertoe leiden dat consumenten geen gebruik zullen maken van de toegang tot de aangeboden content en zullen overwegen om de content 'gratis' te downloaden. Veel content wordt tegenwoordig aangeboden in een relatief gesloten omgeving, waarbij de identiteit van de gebruiker bekend is of via zijn bankgegevens (alsnog) achterhaald kan worden. Ook een account van Facebook, Google of Apple (Apple ID) is steeds beter te herleiden tot de juiste persoon. Vanwege de verschillende pogingen die deze ondernemingen doen om je identiteit te verifiëren zal de betrouwbaarheid hoger zijn dan bij een webwinkel die vooral goederen verkoopt en genoegen neemt met een willekeurig emailadres.[90] Bij deze laatste groep webwinkels is de identiteit vaak van minder groot belang omdat pas na betaling het product wordt geleverd en de zaak daarmee is afgesloten.[91] Ook inlogprocedures via de bestelknop van een telecomaanbieder zoals KPN of ZIGGO zijn vanuit het perspectief van de rechthebbende relatief veilig, maar biedt ook geen volledige garantie. Rechthebbenden die kiezen voor een beveiliging via watermerken als bewijsmiddel zullen in de regel kiezen voor redelijk betrouwbare inlogprocedures waardoor het overgrote deel van de gegevens in de praktijk correct zullen zijn.[92] Aanbieders van content lijken hiermee het gebruiksgemak voor consumenten te laten prevaleren boven een zwaardere beveiliging.

[86] Zie ook par. 4.2.1.2. Zie de eerder genoemde Richtlijn 1999/93/EG en par. 4.2.1.2. Veel genoemde voorbeelden in dit verband zijn DigiD in Nederland en e-ID in België. Bij beide methode blijft het echter de vraag of deze in alle gevallen voldoen aan de eisen van de gekwalificeerde handtekening.
[87] Zie in Nederland Titel 1, afdeling 1A Boek 3 BW en in België Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten.
[88] Zie o.m. Voulon 2013, p. 196.
[89] Dat de (technische) wens van rechthebbende niet leidend is, is ook gebleken uit de inzet van kopieerbeveiliging die uiteindelijk heeft gefaald omdat de eindgebruiker de effecten van de inzet daarvan niet accepteerden. Zie par. 3.2.1.
[90] Zie voor het profileren en identificeren van personen door o.m. Facebook, Roosendaal 2013 (diss.).
[91] Vanzelfsprekend komt ook hier fraude voor door bijvoorbeeld fysieke boeken op een vals adres te laten leveren. Deze boeken worden vervolgens wel opgehaald, maar onder het mom van ' niet afgeleverd' wordt het geld niet betaald of blijkt verdere incasso onmogelijk.
[92] Hierbij kan ook worden gedacht aan de situatie waarin de identiteit weliswaar niet klopt, omdat iemand binnen een huishouden op het gezamenlijke wachtwoord een film heeft besteld. Voor de juridische aansprakelijkheid maakt die wisseling van identiteit op grond van de zorgplicht dan weinig verschil.

Niettemin blijft er een groep over die met onjuiste gegevens zal inloggen om de content te verspreiden.[93] Hierbij kan worden gedacht aan mensen die fictieve namen gebruiken.[94] In dat geval faalt de authenticatieprocedure en is ook een technisch betrouwbaar watermerk niet langer effectief. Dit betekent ook dat het gebruik van watermerken als bewijsmiddel vooral effectief is ten aanzien van afnemers die bereid zijn te betalen en eerlijk hun gegevens ter beschikking stellen. Watermerken als bewijsmiddel houden anders gezegd vooral de eerlijke afnemer eerlijk. Onjuiste gegevens zijn vooral een probleem ten aanzien van het watermerk als opsporings- en bewijsmiddel. In dat geval moet de vraag of het watermerk een juridisch bewijsmiddel kan vormen altijd negatief worden beantwoord. Om als juridisch bewijsmiddel te kunnen dienen zal de rechthebbende tenminste moeten beschikken over voldoende gegevens om iemand als gedaagde of verdachte te kunnen aanmerken. De vraag naar de effectiviteit van het watermerk als juridisch bewijsmiddel begint dan ook pas als de authenticatie tot een aannemelijk resultaat heeft geleid.[95]

2.3 Het proces van watermerken; van aanbrengen tot interpretatie

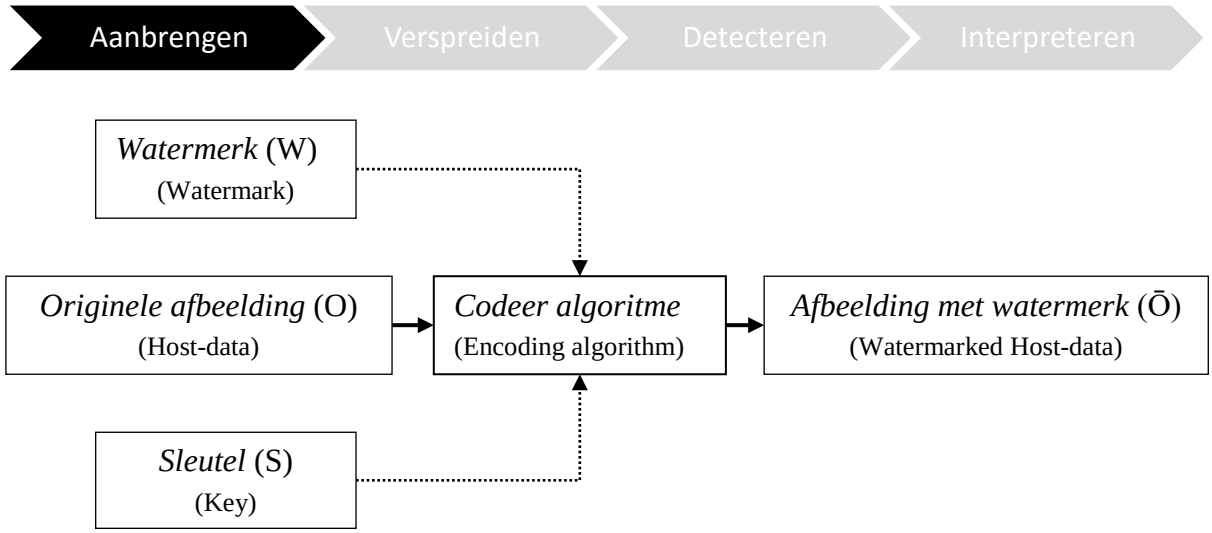
Digitaal watermerken bestaat vanuit een communicatiemodel uit een proces dat wordt onderverdeeld in vier fasen, waarvan de eerste drie in de watermerkliteratuur de meeste aandacht krijgen.[96] De eerste fase bestaat uit het aanbrengen van het watermerk (par. 2.3.1). Daarna volgt de fase waarin het watermerk wordt verspreid (par. 2.3.2) gevolgd door de fase van detectie van het aangebrachte watermerk (par. 2.3.3). Tot slot vindt in de vierde fase de interpretatie plaats (par. 2.3.4). Dit proces van watermerken geldt in beginsel voor iedere vorm van digitaal watermerken. Schematisch kan het proces van watermerken als volgt worden weergegeven.

2.3.1 Aanbrengen

De fase waarin het watermerk wordt aangebracht wordt in de literatuur aangeduid als embedding, insertion of encoding. De standaardwijze om informatie door middel van een

[93] Zie par. 3.2.
[94] Ook iemand die content wil aanschaffen via een webwinkel via een pseudoniem en contact maakt met een anoniem e-mailaccount en daarbij software gebruikt van softwareprogramma's zoals 'Tor' die het mogelijk maken om anoniem gebruik te maken van het internet zal in de praktijk zeer lastig te identificeren zijn.
[95] Twijfels bij de rechthebbende over de juistheid van de gegevens van de licentienemer zal hem er niet snel toe bewegen om een procedure te beginnen. Een procedure brengt immers ook de preventieve werking van het watermerk in gevaar. Zo lang niemand de waarde van het watermerk als juridisch bewijsmiddel test blijft er een angst dat je tegen de lamp kan lopen. Wanneer in een procedure duidelijk wordt dat het watermerk niet (altijd) als juridisch bewijsmiddel kan dienen dan is de rechthebbende direct ook dat voordeel kwijt.
[96] Zie o.m. Craver, Yeo & Yeung 1998, p. 45; Petitcolas, Anderson & Kuhn 1999, p. 1069; Cox e.a. 2008. Watermerken kan in verschillende modellen worden weergegeven. De meest gebruikte zijn het communicatiemodel en het geometrisch model en voor detectie, detectie door correlatie. Vanwege de eenvoud van het communicatiemodel en de toepassing in dit onderzoek wordt het communicatiemodel gebruikt.

watermerk in content te embedden is door data te wijzigen en op die manier toe te voegen aan het gastobject (Host data of cover).[97] Deze data worden door een sleutel (key) in de vorm van een codeeralgoritme (encoding algorithm) gewijzigd en verborgen in een bestand (watermarked cover-data).[98] Wanneer bijvoorbeeld een afbeelding (W) zoals een copyright-teken of een serie nummers door middel van een sleutel (S) als watermerk wordt toegevoegd aan het gastobject (O) dan ontstaat er een nieuwe (gewatermerkte) afbeelding ($\bar{O}$). De sleutel kan een publieke of een geheime sleutel zijn.[99] In de hierna te schetsen situaties wordt uitgegaan van een geheime sleutel. Schematisch kan het embeddingsproces als volgt worden weergegeven ($O \times S \times W \rightarrow \bar{O}$).



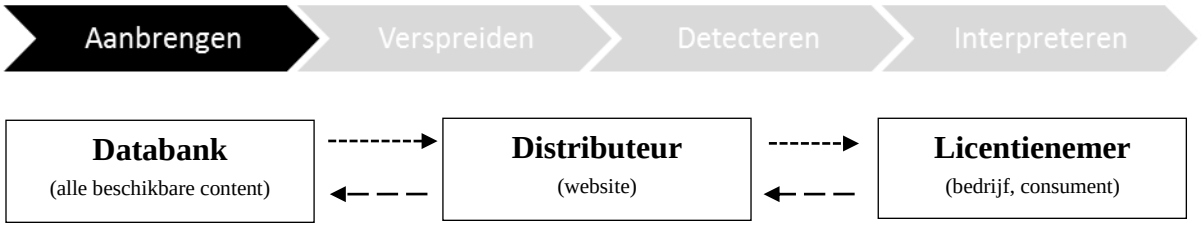
Afhankelijk van de gebruikte techniek en eigenschappen van watermerken is het mogelijk om de functionaliteit van het watermerk te behouden, ook indien een bestand bijvoorbeeld wordt uitgeprint en later weer ingescand.[100] Dit onderzoek richt zich echter op digitale bestanden als zodanig en niet op de verwerking daarvan in fysieke exemplaren.

Bij traitor tracing is het van belang dat het watermerk aangeeft aan wie het betreffende bestand is toegekend. Om bestanden te kunnen verspreiden willen 'piraten' de watermerken in de bestanden opsporen en aanvallen. Een aanval waarbij meerdere personen hun bestanden delen om het watermerk zichtbaar te maken en aan te vallen wordt ook wel omschreven als een collusion-attack (par. 2.5). Door bestanden met een watermerk te vergelijken kunnen zij de verschillen en daarmee het watermerk aan het licht brengen. Vervolgens zullen zij op die plaatsen het watermerk proberen aan te vallen. Om watermerken resistent te maken tegen

[97] Het originele object wordt in de literatuur op verschilde wijze weergegeven. Stego-image (Petitcolas, Anderson & Kuhn 1999, p. 1064; Cover data (Katzenbeisser & Petitcolas 2000, par. 5.2.2, p. 101; Host data (Langelaar, Setywan & Lagendijk 2000, p. 21); Host-Signal of Cover-object (Li & Memon 2007, p. 60); Cover Media (Cox e.a. 2008, p. 2).
[98] Voor het gewatermerkte bestand worden ook een aantal termen gebruikt: Marked image (Petitcolas, Anderson & Kuhn 1999, p. 1065); Watermarked data (Langelaar, Setywan & Lagendijk 2000, p. 21) ; Watermarked Work of Stego Work (Cox e.a. 2008, p. 3).
[99] Vgl. ook de elektronische handtekening. Zie daarvoor o.m. Kemna 2004, p. 205; Dondorp 2011; Voulon 2014.
[100] Dit geldt niet altijd en is sterk afhankelijk van de gebruikte techniek.

deze aanvallen zal de rechthebbende wensen dat het watermerk bestand is tegen zoveel mogelijk aanvallers (in de regel geldt hoe groter de groep hoe lastiger iemand te traceren is), een zeer lage kans geeft op valse beschuldigingen (fout-positief), een zeer lage kans om helemaal niemand te kunnen traceren (fout-negatief) en bij voorkeur met een code die gunstig is bij een trade-off met andere eigenschappen (par. 2.4). In de literatuur wordt steeds gezocht naar het beste resultaat.[101] Voorlopig wordt de traitor tracingscodes van Tardos als beste gezien en wordt daar verder aan gewerkt. Deze codes kunnen collusion attacks overleven en met grote zekerheid achterhalen wie met wie samenwerkte met bovendien een heel kleine kans dat een onschuldige wordt aangeduid.

In de praktijk zal het model er zo uit zien dat de licentienemer zich via de distributeur, zoals een webwinkel, kenbaar maakt bij de aanschaf van de content, waarna zijn gegevens in een databank worden opgenomen en van een corresponderende code worden voorzien die wordt opgenomen als boodschap (watermerk). Vanuit privacyoverwegingen zal men deze code veelal opmaken als een niet tot een natuurlijk persoon herleidbare code.[102] Nadat het watermerk is aangebracht kan de distributeur de content uitleveren. In praktijk zal het gebruik van watermerken moeten aansluiten bij de wens van zowel de eindgebruiker als de politiek om content op een eenvoudige wijze aan te kunnen schaffen.[103] Watermerken (de algoritmen) moeten met andere woorden snel genoeg (on the fly) kunnen worden aangebracht. Daarnaast maakt dit schema duidelijk dat de gegevens die de licentienemer ter beschikking stelt betrouwbaar moeten zijn. In tegenstelling tot fysieke producten hoeven deze producten niet te worden afgeleverd op een fysiek adres waardoor de noodzaak bij de eindgebruiker ontbreekt om de juiste gegevens op te geven.[104] Het succes van watermerksystemen is mede afhankelijk van de invoer van de juiste gegevens. Dit probleem speelt bij veel meer toepassingen van e-commerce een rol. Daarbij zal een afweging moeten worden gemaakt tussen beveiliging en gebruiksgemak. Beveiliging zal men bij digitale exemplaren sneller gewenst achten dan bij fysieke exemplaren, omdat bij digitale content ook een kleine groep mensen op een eenvoudige wijze snel een grote illegale distributie op gang kan brengen.[105]



[101] Zie Boneh & Shaw 1998; Tardos 2003; Furon & Perez-Freire 2009; Charpentier e.a. 2011
[102] De vraag is dan voor wie de betreffende code al dan niet herleidbaar is tot de natuurlijke persoon. Zie voor aspecten van privacy par. 5.3.1.
[103] Zie voor deze wensen o.m. het green paper 'online distribution of audiovisual works in the European Union: opportunities and challenges towards a digital single market' Brussels, 13.7.2011, COM(2011) 427.
[104] Ook bij fysieke producten worden overigens onjuiste adressen genoteerd. Fraude valt in die zin nooit helemaal uit te sluiten.
[105] Zie o.m. par. 3.2.1. Dit argument wordt vooral bij e-boeken veelgebruikt en zorgt voor terughoudendheid bij uitgevers bij het ontwikkelen van online-distributiemodellen.

2.3.2 Verspreiden

Wanneer een watermerk in het gastobject is aangebracht, is het klaar om verspreid te worden. Deze gewatermerkte bestanden kunnen door verschillende kanalen worden verstuurd, zoals de kabel (Pay-TV), internet (website, streaming) of een printer (poster). In deze fase staat het bestand inclusief het watermerk ook bloot aan verschillende aanvallen of verstoringen. Deze aanvallen kunnen malafide zijn doordat een aanvaller opzettelijk het watermerk wil aantasten, verwijderen of ondetecteerbaar wil maken. Het is echter ook mogelijk dat een aanval voortkomt uit normaal gebruik. Zo verandert het bestand van een digitale foto ook wanneer deze van formaat wordt veranderd, bijvoorbeeld doordat het bestand is gecomprimeerd. Samenvattend kan het watermerk op twee verschillende wijze worden aangevallen. Ten eerste door normaal gebruik. Bijvoorbeeld omdat de eindgebruiker de foto comprimeert of roteert. Ten tweede door een malafide aanval met als doel het watermerk aan te tasten, te verwijderen of ondetecteerbaar te maken. Een van de uitdagingen is dan om het watermerk zo te ontwerpen dat het weerstand kan bieden tegen de meest voorkomende aanvallen of verstoringen en detecteer blijft.[106]

2.3.3 Detecteren

Om de boodschap (het watermerk) te kunnen uitlezen zal het watermerk eerst moet worden gevonden. Voor het detecteren van een watermerk moeten drie stappen worden genomen; opsporing van het gastobject, detectie van het watermerk en de decodering van het watermerk.

Ten eerste moet het gastobject worden opgespoord.[107] Het gastobject in de vorm van bijvoorbeeld een film kan per toeval worden gevonden of door specifieke handmatige of geautomatiseerde zoekopdrachten. De rechthebbende kan dit zelf doen of uitbesteden aan zogeheten Watermarking Search Services (WSS), die het gehele proces als een service aanbieden.[108]

Ten tweede moet het watermerk worden opgespoord (detection). De eerstgenoemde stap van het opsporen van het gastobject wordt in de watermerkliteratuur niet altijd expliciet genoemd. Vaak wordt over detectie van het watermerk gesproken waarbij de opsporing van het bestand zelf dan al wordt verondersteld.[109]

De eerste stap wordt vaak uitgevoerd met behulp van verschillende softwareprogramma's, zoals webcrawlers die op het internet zoeken naar bestanden met behulp van de naam van een film of muzieknummer, trefwoorden, logo's en andere metadata.[110] Hoewel deze webcrawlers

[106] TNO 2011, p. 31.
[107] Zie over de opsporing daarvan in het bijzonder Steinbach & Wolf 2008.
[108] Steinbach e.a. 2010.
[109] Zie bv. Cox e.a. 2008, p. xxi.
[110] Zie o.m. Steinebach e.a 2010, p. 154. Zo spoorde de webcrawler SINBAD van Librius, de beheersvennootschap van de Vlaamse boekenuitgevers, in de zomer van 2011 naar eigen zeggen 29 duizend links naar illegale ebooks en strips op en is het in staat 25.000 webpagina's per dag te doorzoeken. Zie http://www.boekenvak.be/nieuws/sinbad-de-eerste-belgische-anti-piracy-webcrawler-voor-boeken-en-strips-haalde-al-29000-illeg; http://www.librius.com/over-librius/wat-doet-librius/Librius-SINBAD/

steeds geavanceerder worden blijft het lastig om afbeeldingen, films of audio te vinden die zijn aangepast. Zo is het eenvoudig om de naam van een bestand te wijzigen, maar veranderen ook veel metadata van bijvoorbeeld een foto als je een bestandsformaat wijzigt van JPEG naar PNG.[111] Door er een screenshot van te maken blijven er helemaal geen metadata meer over. Andere programma's maken gebruik van software die op internet zoekt naar dezelfde foto's. Vaak wordt er dan gebruikt gemaakt van een originele foto en gaat het programma op zoek naar foto's die overeenkomen.[112] Beperkingen ten aanzien van de opsporing van inbreukmakend content worden voor een belangrijk deel gecompenseerd door de aard van de content die wordt gezocht. Content die door de rechthebbende van een watermerk is voorzien heeft in het kader van zoekstrategieën als voordeel dat het voor de illegale aanbieders vooral waarde vertegenwoordigt wanneer het eenvoudig kan worden gevonden.[113] Het zoeken naar zuiver inbreukmakende content (letterlijke kopieën) wordt daarmee vereenvoudigd.[114] Een film of een bepaalde audio track moet immers als zodanig bekend zijn om ook door anderen te kunnen worden gevonden. Werken waarin andere werken zijn verwerkt zijn lastiger te vinden. Zo zal het in beginsel lastig zijn een fotocollage op te sporen. Op You Tube zijn verschillende filmpjes te vinden waarin een compilatie is gemaakt van auteursrechtelijk beschermde foto's, vaak ondersteund met een audio-track of een compilatie daarvan. Vaak zijn deze foto's bewerkt (snijden, verkleinen). Ook hier geldt dat mensen zelf in het informatieveld of anderen in de commentaren wel sporen achter laten door het benoemen van bepaalde foto's of het opgenomen muziekfragment.

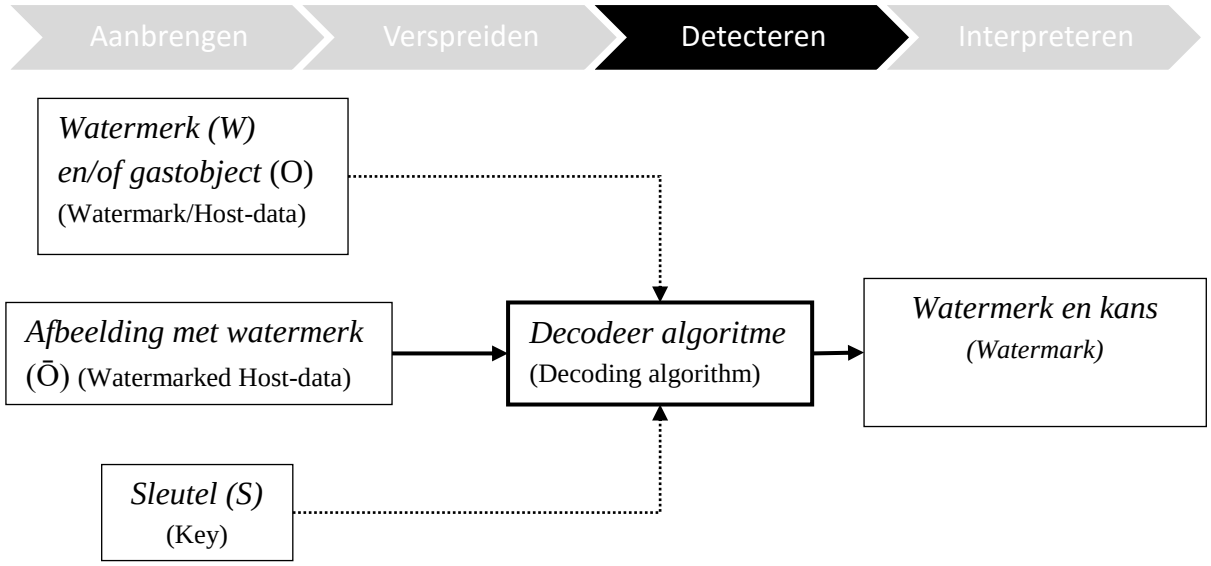
Een ander probleem bij het detecteren van inbreukmakende bestanden is dat de er sprake is van veel vervuiling doordat ook opsporingsinstanties zelf nep-content op internet plaatsen.[115] Hierdoor nemen de zoekkosten toe omdat zelfs na de detectie de vangst nog enkel kan bestaan uit een collega-opspoorder. Een goede afstemming tussen de private handhavers is hierdoor gewenst.

Nadat het gewatermerkte bestand is opgespoord kan het watermerk worden gedetecteerd door gebruik te maken van een decodeeralgoritme (decoding algorithm) met de sleutel die is gebruikt bij het coderen of aanbrengen van het watermerk.[116] Het uitlezen van het watermerk

[111] JPEG of JPG (Joint Photographic Experts Group) en PNG (Portable Network Graphics) zijn bestandsformaten voor afbeeldingen die het mogelijk maken om met weinig kwaliteitsverlies een bestand relatief klein te houden.
[112] Zie bijvoorbeeld 'search by image' van google: http://www.google.com/insidesearch/searchbyimage.html.
[113] In vergelijking met o.m. kinderporno dat lastiger te vinden is. Zie o.m. Cuevas e.a. 2011, p. 7 en par. 3.2.2.
[114] In de praktijk zal men zich richten op de grote bronnen waartoe een grote groep eindgebruikers toegang heeft. Lastig toegankelijke en weinig bezochte subdomeinen zullen om die reden veelal buiten schot blijven. Voor het opsporen van letterlijke kopieën wordt ook veel gebruik gemaakt van hashtechnieken, o.m. door Getty Images.
[115] Zie o.m. het onderzoek dat Cuevas e.a. 2011 uitvoerde.
[116] Afhankelijk van de wijze waarop het watermerk is aangebracht en de aard van het watermerkalgoritme kan de detectiemethode van het watermerk op verschillende wijze plaatsvinden. Zo kan een watermerk in zijn exacte vorm worden onttrokken uit de content (watermark extraction) bijvoorbeeld wanneer een logo was verstopt in een foto en deze in zijn geheel zichtbaar wordt gemaakt. Ook is het denkbaar dat een robuuste hashfunctie in een foto is opgenomen en deze geëmbedde hash waarde later aan de afbeelding wordt onttrokken en vergeleken om te kijken of de afbeelding authentiek is of significant is aangepast. Een andere wijze van detectie die kan worden onderscheiden is die wanneer een bepaald signaal (signal) in content is opgenomen (watermark detection) en

zal dan moeten leiden tot de boodschap die eerder als watermerk is aangebracht. Het bewijs zal bij traitor tracing veelal bestaan uit een kansberekening die, evenals bij DNA-bewijs, duidelijk maakt hoe groot de kans (of hoe waarschijnlijk het) is dat het specifieke watermerk dat is aangetroffen in het gastobject toebehoort aan de licentienemer en niet aan een ander.

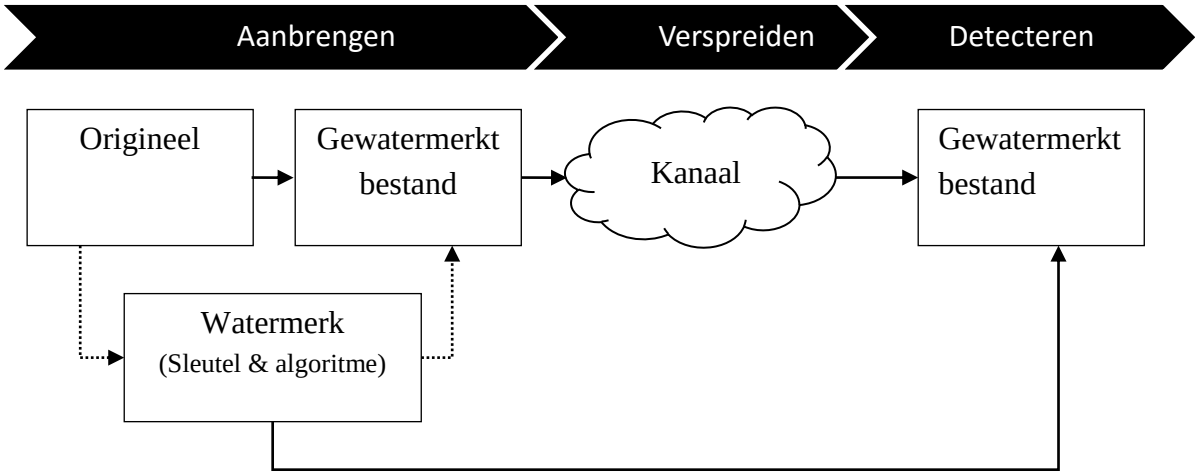
Voorkomen moet worden dat er een fout-positief of false-positive ontstaat. Dit ontstaat wanneer het detectiealgoritme een code 'detecteert', die niet in het werk werd gestopt. Een dergelijke verwarring kan ontstaan doordat de detectiealgoritmen zelf ook werken op basis van kansberekening. Deze algoritmen geven dan aan dat het 'het meest waarschijnlijk is dat de onderstaande code in het werk zit'. Aan deze antwoorden worden door de onderzoekers grenzen gesteld, zodat het antwoord 'heel zeker' wordt. Het detecteren van een watermerk kan schematisch als volgt worden samengevat:



Uiteindelijk zal het watermerk afhankelijk van het gebruikte detectiesysteem in het gastobject worden gedetecteerd met behulp van een algoritme en sleutel. Dit leidt uiteindelijk tot dezelfde boodschap (watermerk) of een kansberekening ten aanzien van de boodschap (confidence measure). Er kunnen ook meerdere watermerken worden aangebracht in een gastobject. Indien meerdere watermerken zijn aangetast zou nog berekend kunnen worden hoe groot de kans is dat het watermerk toebehoort aan een bepaalde licentienemer. Samenvattend bestaat de detectiefase uit drie stappen. Het vinden van het gastobject, het detecteren van het watermerk in het gastobject en het decoderen van het gevonden gastobject. In de regel vindt de opsporing van het gastobject plaats door zogeheten webcrawlers die hiervoor het internet afzoeken.

Het proces van watermerken van origineel tot detectie van het watermerk kan daarmee als volgt worden weergegeven.

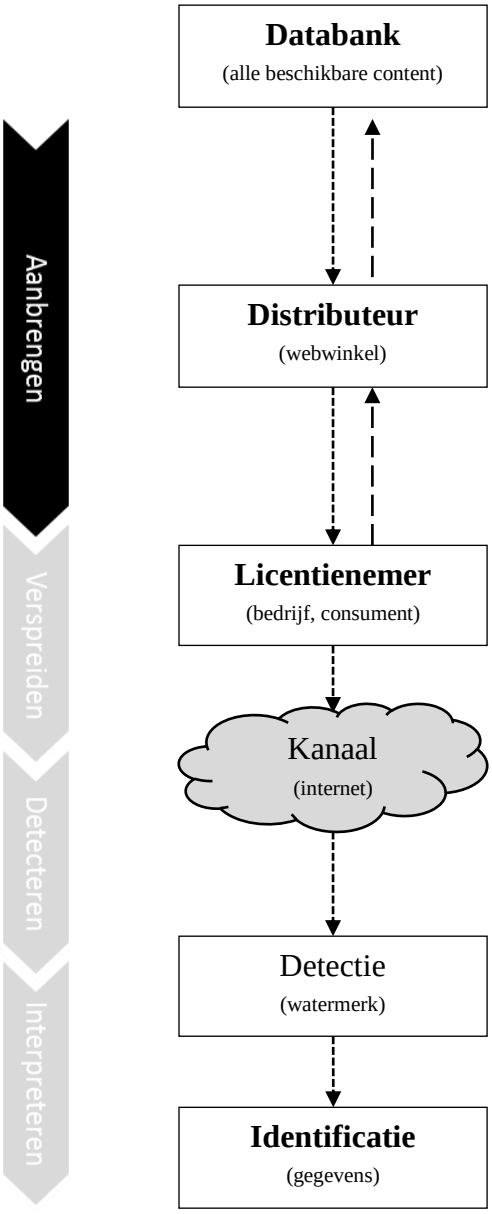
slechts bedoeld is voor detectie doelen, zoals het geval is bij bijvoorbeeld het monitoren van reclameuitzendingen, waarna er per uitgezonden reclameboodschap afgerekend kan worden.



Om onnodige toegang tot de persoonsgegevens van de licentienemer te voorkomen en daarmee zijn privacy te beschermen is het raadzaam om de databanken met de ID te scheiden van de persoonsgegevens van de licentienemer.[117] De databank met persoonsgegevens moet in dat geval door een Thrusted Third Party (TTP) worden beheerd, die slechts toegang geeft nadat inbreuk is vastgesteld door de rechthebbende. Hiermee kan onder andere worden voorkomen dat volledig geautomatiseerd mensen worden aangeschreven zonder dat er inbreuk is vastgesteld, bijvoorbeeld doordat er sprake is van een wettelijke of contractuele uitzondering.[118]

In de praktijk zal het model er zo uit zien dat de licentienemer zich via de distributeur kenbaar maakt bij de aanschaf van de content, waarna zijn gegevens in een databank worden opgenomen en van een corresponderende code worden voorzien die wordt opgenomen in het watermerk. Wanneer de content daarna op internet wordt gevonden en het watermerk kan worden gedetecteerd, geïnterpreteerd en de code vervolgens succesvol aan de licentienemer kan worden gekoppeld dan kan deze eventueel worden aangesproken. Schematisch ziet het model erop de volgene pagina als volgt uit.

[117] Zie par. 5.3.3.1.
[118] Zie voor de inbreukcriteria in het auteursrecht par. 3.4. De grenzen van het dreigen met beweerdelijke auteursrechten is volgens vaste rechtspraak gelegen in het onrechtmatig handelen van eiser door tot handhaving over te gaan terwijl hij behoort te weten dat hij hiertoe het recht niet heeft.



De door bijvoorbeeld een webwinkel te distribueren content is opgeslagen in een databank. Wanneer een klant van de webwinkel content wil aanschaffen dan vraagt hij juridisch gezien toestemming aan de rechthebbende die in ruil voor een vergoeding hem daarvoor een licentie verschaft.[119]

De gegevens die nodig zijn voor het sluiten van de overeenkomst, zoals de naam en bankrekeningnummer voor de betaling worden omgezet in een code die correspondeert met de gegevens van de klant. De vraag is dan voor wie de betreffende code al dan niet herleidbaar is tot de natuurlijke persoon. In de literatuur is in het kader van de betrouwbaarheid van het bewijs ook wel gesuggereerd hiervoor een TTP te gebruiken, zodat

[119] Ik treed hier niet in de discussie of het aanschaffen van content slechts een licentie-overeenkomst is dan wel als koop kan worden gekwalificeerd. Zie voor softwarebetrekkingen tussen de auteur, de verkrijger en hun vermogensrechtelijke positie jegens derden, o.m. Nepelenbroek 2013 (diss.).

ook de rechthebbende en distributeur niet weten welke code het watermerk dat in het werk is aangebracht bevat. In dat geval stuurt de rechthebbende of distributeur de gegevens naar de TTP die deze gegevens vervolgens bewaart en deze gegevens omzet in een code en deze als boodschap aan het watermerk meegeeft. Vervolgens kan de TTP zelf of via een beveiligde verbinding het watermerk in de content plaatsen en kan de content aan de licentienemer worden uitgeleverd. Voor dit proces zijn nog meer benaderingen denkbaar. Belangrijk in dit proces is dat de distributeur of rechthebbende niet rechtstreeks toegang heeft tot de code om te voorkomen dat bij het presenteren van het bewijs het argument naar voren wordt gebracht dat de code die verwijst naar de licentienemer later is aangebracht door de distributeur of rechthebbende. Daarnaast biedt dit proces enkele privacyrechtelijke voordelen voor zowel de eindgebruiker als de rechthebbende.[120] Door zorgvuldig om te gaan met de privacy van de licentienemer kan de rechthebbende voorkomen dat het watermerk als onrechtmatig verkregen bewijs wordt aangemerkt.

2.3.4 Interpretatie

De laatste fase is die van de interpretatie van het watermerk waarin de vertaalslag plaatsvindt tussen de code die gedetecteerd is en de betekenis daarvan. Voor de interpretatie van watermerken is in de watermerkliteratuur weinig aandacht, anders dan in de vorm van aanvallen die tot doel hebben tot een false-positive te leiden of het onmogelijk maken een watermerk te detecteren.[121] De interpretatie van watermerken in het geval van traitor tracing zal in de regel bestaan uit statistiek in de vorm van kansberekening. Over het gebruik van statistiek ten behoeve van bewijsvoering is het een en ander geschreven in de forensische literatuur zoals bij DNA-bewijs. Het gaat daarbij niet alleen om de toelaatbaarheid van statistiek als bewijs maar ook om valkuilen bij de interpretatie van dergelijk bewijs en het voor rechters onvermijdelijke gebruik van experts. Daarover meer in hoofdstuk 4 en hoofdstuk 6.

2.3.5 Tussenconclusie: risico’s ten aanzien van de betrouwbaarheid

Voor het beoordelen van de prestaties van een watermerksysteem is een aantal zaken van belang, zoals de kans op vals alarm bij detectie, de kans op detectie wanneer de aanwezigheid van het watermerk wordt getest en de kans op fouten wanneer de boodschap wordt geëxtraheerd.[122] Om het watermerk uiteindelijk als juridisch bewijsmiddel te kunnen gebruiken zijn naast de juridische vragen van toelaatbaarheid de vragen naar de betrouwbaarheid van het watermerksysteem van belang. Uit het hier weergegeven proces kan een aantal risico’s worden gedistilleerd. In ieder van de drie fasen zijn er momenten te onderscheiden waarop de betrouwbaarheid van het watermerk (boodschap) kan worden aangetast.

[120] Zie par. 5.3.
[121] Zie o.m. Craver e.a. 1998, p. 52.
[122] Zie o.m. Hernandez & Perez-Gonzalez 1999.

In de eerste fase is er een aantal risico's te onderscheiden. Voor het watermerk als effectief bewijsmiddel is van belang dat aangetoond kan worden dat de bij de bewijsvoering getoonde originele foto ook daadwerkelijk een originele foto is en niet achteraf op de server gewijzigd is.[123] Dat betekent dat voorkomen moet worden dat de rechthebbende het watermerk er ook achteraf in kan zetten door de sleutel op zodanige wijze aan te passen dat de gewenste boodschap er in staat. Het is immers niet alleen mogelijk er met behulp van een algoritme en sleutel een watermerk in te stoppen, maar dit kan in theorie ook andersom. Met een geschikt gekozen sleutel kan elke gewenste informatie uit een bestand worden gehaald. Dat betekent dat iemand onrecht kan worden gezien als maker van een werk, maar het kan ook betekenen dat je een licentie toewijst aan iemand die er nooit een heeft gehad. Dit is naast een technische uitdaging ook een organisatorische uitdaging. Het komt daarbij aan op vragen die samen hangen met toegang tot de sleutels en andere beveiligingsvraagstukken. Om de vraag te beantwoorden of de sleutel uiteindelijk vervalst is moet gekeken worden naar de vraag hoe moeilijk het is om een dergelijke sleutel te vervalsen. Daarbij speelt onder meer de vraag hoeveel rekenkracht er nodig is en of het praktisch mogelijk is. In die gevallen zal vastgesteld moeten worden hoe waarschijnlijk het is dat de sleutel vervalst is. In de literatuur is al vaker op dit probleem gewezen. Er wordt dan ook op gewezen dat het voor de betrouwbaarheid beter zou zijn de codes (sleutel en algoritme) eventueel inclusief de originele foto door een onafhankelijke derde te laten registeren. Die derde zou dan een rol kunnen spelen die vergelijkbaar is met die van een Trusted Third Party (TTP) bij een elektronische handtekening.[124] De gedachte om een TTP een rol geven speelt al vanaf het begin van de opkomst van het watermerk in de literatuur.[125] Op dit moment bestaat er echter nog geen TTP die deze dienst aanbiedt. Een mogelijke reden kan zijn dat een TTP in een commerciële omgeving te duur is in verhouding tot de te verwachten resultaten. De vraag naar een TTP doet zich in de praktijk immers alleen voor wanneer een partij het watermerk in een rechtszaak betwist en een succesvolle betwisting naar verwachting in de toekomst tot meer problemen leidt. Voor de juridische praktijk betekent dit dat er twijfels kunnen worden geuit ten aanzien van de betrouwbaarheid. Om die twijfel weg te nemen zal er in ieder geval een deskundige een oordeel moeten geven over de vraag hoe waarschijnlijk het is dat de sleutel is vervalst. In de handhavingspraktijk hoeft dit niet direct gevolgen te hebben, omdat ook watermerken waarvan de betrouwbaarheid betwist kan worden een voldoende afschrikwekkend effect kunnen hebben. Het hoeft immers geen betoog dat veel van de handhavingsdynamiek zich buiten de rechtszaal afspeelt.

In de tweede fase vormt, afhankelijk van het type watermerk dat is ingezet, de robuustheid van een watermerk een risico voor de betrouwbaarheid. Bij het verspreiden en het gebruik van het gewatermerkte bestand kan het bestand op verschillende wijzen worden aangetast. Dit kan

[123] Het specifieke aan watermerken is dat de 'code van het watermerk', wordt geëmbed door wijzigingen aan te brengen in het origineel. Zonder het origineel ken je de wijzigingen niet en moet je dus op zoek naar structuren om bepaalde informatie te lezen. Hiervoor heb je dus al de sleutel nodig en toegang tot het decoderingsalgorithme.
[124] Zie o.m. Van Esch 2007, p. 125.
[125] Er wordt echter ook nagedacht over protocollen die zonder een TTP werken. Zie o.m. Choi e.a. 2003.

door aanvallen als gevolg van normaal gebruik, zoals het vergroten, verkleinen of het snijden van bijvoorbeeld een foto, maar ook door malafide aanvallen op het watermerk. In dit laatste geval valt iemand met opzet het gewatermerkte bestand aan met als doel het watermerk aan te tasten of te verwijderen. Zowel bij het ontwerp als de inzet van watermerken zal hiermee rekening moeten worden gehouden. De meeste robuuste watermerken kunnen weerstand bieden tegen de aanvallen als gevolg van gebruik. Ten aanzien van de malafide aanvallen zal men duidelijk moeten maken tegen welke aanvallen het watermerk, gegeven de toepassing in die situatie, weerstand kan bieden en tot slot hoe waarschijnlijk het is dat er een aanval is uitgevoerd die de betrouwbaarheid van de boodschap heeft aangetast.

In de derde fase en vierde fase is het van belang dat de detectie en interpretatie op een zorgvuldige wijze wordt uitgevoerd en dat hier een duidelijke verslaglegging over plaatsvindt. Dat betekent dat niet alleen het systeem technisch voldoende gewaarborgd moet zijn maar ook de organisatie daarom heen. Om later antwoorden te kunnen geven op vragen die in de juridische procedure naar voren komen is het van belang dat de organisatie zo in elkaar zit dat deze informatie op elk moment beschikbaar is.

Tot slot laat het proces zien dat de sleutel een belangrijke rol speelt. Als de sleutel bekend is bij de aanvaller dan is in beginsel de code gekraakt en kan eenvoudig inzichtelijk worden gemaakt waar de wijzigingen die het watermerk vormen zich bevinden. Het is dan verder een kleine stap om het watermerk te wijzigen of te verwijderen. Enkele risico's zijn hiervoor beschreven. Een ander en meer algemeen risico is gelegen in de aard van watermerken. Door het gebruik van verschillende wiskundige modellen bij zowel het proces van aanbrengen van het watermerk als bij de detectie en interpretatie daarvan vormt ook het gebruikte wiskundig model een risico. Het aanvallen van het onderliggende model kan kansen bieden om de betrouwbaarheid van het watermerk ter discussie te stellen. Bijvoorbeeld door het gebruikte model aan te vallen dat is gebruikt om het watermerk te embedden. Ook daarvoor geldt dat een goede onderbouwing van het model voor handen moet zijn.

2.4 Eigenschappen van watermerksystemen en -technieken

Watermerken maken gebruik van verschillende eigenschappen, zoals waarneembaarheid, capaciteit, robuustheid en beveiliging.[126] Deze eigenschappen zijn niet altijd complementair maar vormen vaak een trade-off die voor een belangrijk deel afhankelijk is van de gewenste toepassing. Zo is de capaciteit van het watermerk van invloed op de waarneembaarheid ervan. Bij de inzet van watermerken zal men derhalve keuzes moeten maken in de functie van het doel dat men met de inzet van het watermerk beoogt te bereiken.[127] Een uniform pakket van eisen is om die reden dan ook lastig te geven. In deze paragraaf worden verschillende

[126] Petitcolas, Anderson & Kuhn 1999; Hartung & Kutter 1999; Langelaar, Setywan & Lagendijk 2000, p. 21. Cox, e.a. 2007, p. 36 onderscheiden er tien. Een aantal van deze eigenschappen is door mij vanwege het overzicht samengebracht in paragraaf 2.4.1 (embedden en detectie).
[127] Zie o.m. Langelaar, Setywan & Lagendijk 2000, p. 22. Voor de doelen zie par. 2.2.4.

eigenschappen besproken die van invloed zijn op de keuze voor een bepaalde watermerktechniek. Men mag immers niet vergeten dat de keuzes die zijn gemaakt van invloed zijn op de betrouwbaarheid van het watermerk als bewijsmiddel. Daarnaast heeft deze paragraaf als doel de verschillende onderwerpen van de (huidige) watermerkliteratuur, veelal in de vorm van papers, een plaats te geven voor juristen. Voor uitgebreidere informatie (over elkaar bijtende eigenschappen van watermerken) wordt verwezen naar andere literatuur.[128] De eerste twee subparagrafen over detectie en embedden (zie hieronder) sluiten aan bij de eerder in paragaaf 2.3 genoemde fasen. De subparagrafen behandelen enkele keuzes ten aanzien van technieken die worden gebruikt bij het embedden en detecteren van watermerken. Deze paragraaf begint met een beschrijving van detectiesystemen omdat de keuze voor een embed- en detectie-algoritme onder meer afhankelijk is van de wijze van detectie. [129] De daarop volgende paragrafen behandelen keuzes die gemaakt moeten worden ten aanzien van achtereenvolgens de waarneembaarheid, capaciteit, robuustheid en beveiliging. De laatste eigenschap die wordt besproken betreft de keuze ten aanzien van kosten van watermerken. Voor het overzicht wordt de paragraaf afgesloten met enkele conclusies.

2.4.1 Detectie

Ten aanzien van de detectie van watermerken worden in de literatuur drie soorten watermerksystemen onderscheiden. Het onderscheid ziet op de vraag wat er nodig is om het watermerk te extraheren.[130] Ten eerste de zogenoemde private of non-blind watermerk-systemen.[131] Deze systemen maken voor de detectie van het watermerk gebruik van het (niet gewatermerkte) origineel of informatie daaruit en wordt ook wel aangeduid als geïnformeerde detectie (Informed Detection).[132] Het (non-blind) detectie-algortime heeft met andere woorden een directe toegang nodig tot het originele bestand en is derhalve ook alleen te gebruiken wanneer toegang tot het origineel mogelijk is. Dit betekent in de regel dat er een databank nodig is. Deze detecteeralgoritmen worden in de literatuur afgekort tot non-blind detection. In relatie tot de andere nog te noemen systemen zijn deze het meest robuust. Voor een aantal applicaties of toepassingen is een dergelijk systeem echter niet mogelijk of wenselijk.[133] Dit geldt met name voor grote collecties waarvoor dan tevens alle originele bestanden moeten worden bewaard in een databank en kunnen worden opgeroepen bij de detectie. Dit vereist de nodige opslagcapaciteit. Zo is het bijvoorbeeld bij video niet praktisch

[128] Zie voor een overzicht o.m. Raj & Ali 2012; Cox e.a. 2008 die in bijna 600 pagina's meerdere systemen van watermerken beschrijven. Veel watermerkliteratuur is in de vorm van papers ook online raadpleegbaar.
[129] Zie voor voorbeelden en overzichten van algoritme o.m. Cox e.a. 1997; Swanson, Kobayashi & Tewfik 1998; Wang, Doherty & Dyck 2002; Shieh e.a. 2003 ; Cox, e.a. 2007, p. 137.
[130] Kutter & Petitcolas 1999, p. 227; Katzenbeisser & Petitcolas 2000, par. 5.3, p. 103; Langelaar, Setywan & Lagendijk 2000, p. 22.
[131] Ook aangeduid als Nonoblivious watermarking (Langelaar 2000 (diss.) par. 1.2, p. 4; Langelaar, Setywan & Lagendijk 2000, p. 22.).
[132] De terminologie van privaat en publiek refereert de toepassing van het watermerksysteem en daarmee naar de vraag of een selecte (private) in staat moet worden gesteld om het watermerk te detecteren of dat iedereen (public) moet kunnen. Omdat originele objecten in beginsel alleen beschikbaar zijn bij private toepassingen kan de informed detection niet plaatsvinden in bij publieke watermerksystemen.
[133] Kutter & Hartung 1999; Katzenbeisser & Petitcolas 2000.

om gebruik te maken van de originele film omdat daarvoor een (te) grote hoeveelheid data moet worden verwerkt.

Een tweede type systeem is de semi-blind of semi-private. Dit systeem maakt voor het antwoord op de vraag of het gast-object een watermerk bevat geen gebruik van het origineel maar enkel van het gewatermerkte bestand.[134] Beide systemen kunnen en worden mede vanwege de robuustheid toegepast voor het bewijs van eigendom (authenticiteit) en fingerprinting voor identificatie van de licentienemer of gepirateerde kopieën.

Het laatste en derde type watermerksysteem is het zogenoemde blinde of publieke watermerksysteem waarbij zowel het origineel als het gewatermerkte gastobject niet nodig zijn om de eerder genoemde vraag naar detectie van het watermerk op te lossen (blind detection).[135] Deze techniek wordt met name ingezet voor kopieerbeveiliging, indexering en tracering. De (blind) extractie-algoritmen hebben in dit geval geen toegang nodig tot het origineel en worden in de literatuur afgekort tot blind detectors.

Watermerksystemen die, zoals in dit onderzoek, het mogelijk moeten maken om veel bestanden snel van een watermerk te voorzien en te kunnen detecteren en bedoeld zijn voor de authenticatie en tracing zullen in de regel gebruik maken van semi dan wel blinde of publieke watermerksysteem en daarbij gebruik maken van blind detection. Dit gaat weliswaar ten koste van de robuustheid, maar bespaart op de aanwezigheid van het origineel en maakt een hogere detecteersnelheid mogelijk. Voor de toepassing hiervan op het internet is het van belang dat wanneer er bij de opsporing van (vermeend) inbreukmakend materiaal gebruik wordt gemaakt van applicaties zoals webcrawlers de extractie van het watermerk niet te complex mag zijn om het watermerk snel en goed uit te kunnen lezen.

Een succesvol watermerk is uiteindelijk een watermerk dat na detectie resulteert in een (positieve) detectie.[136] De effectiviteit van het systeem is de kans op detectie na embedding en voor latere verstoringen, zoals aanvallen of transmissie (effectiveness rate). Een honderd procent score is alleen mogelijk tegen hoge kosten in relatie tot de andere eigenschappen. Afhankelijk van de gewenste toepassing zal de gebruiker een afweging moeten maken. Zo zal een website, die duizenden foto's per dag wil voorzien van een watermerk om later duidelijk te kunnen maken wie als rechthebbende is aan te merken (proof of ownership), hoge eisen stellen aan de (on)waarneembaarheid van het watermerk.[137] Wanneer men zou besluiten om watermerken in te zetten zal men een keus moeten maken tussen het toestaan van meer verstoring of meer effectiviteit in de vorm van een hogere kans op detectie. De effectiviteit

[134] Dat betekent dat de uitgever van het watermerk voor de detectie een kopie van het gewatermerkte bestand moet bewaren. Ook bij deze systemen zijn er referentiecijfers nodig maar deze zijn in aantallen veel kleiner dan bij niet-blinde technieken.
[135] Ook aangeduid als Oblivious watermarking door Langelaar 2000 (diss.), p. 4; Langelaar, Setywan & Lagendijk 2000, p. 22.
[136] Zie o.m. Cox, e.a. 2008, p. 37.
[137] Zie hierna par. 2.4.3 verwaarneembaarheid.

kan op een aantal wijzen worden gemeten, zoals analytisch of empirisch door een serie testen uit te voeren bij een serie foto's die vanzelfsprekend voldoende representatief moet zijn en uitgevoerd in het verwachte of gebruikte proces.[138]

Een ander belangrijk aspect van detectie betreft zoals eerder genoemd, de zogenoemde fout-positief of false positive.[139] Bij een fout-positief geeft de detector ten onrechte aan dat het object een watermerk bevat. Het aantal te verwachten fout-positieven in een bepaald aantal runs van de detector wordt aangeduid met de term 'fals positive rate'.[140] Een dergelijke verwarring kan ontstaan doordat de detectiealgoritmen zelf ook werken op basis van kansberekening. Aan de mate van zekerheid worden door de onderzoekers grenzen gesteld, zodat het antwoord 'heel zeker' wordt. Aan de hand van verschillende parameters kan de rechthebbende tot een zekere hoogte zelf bepalen wat de kans is op een fout-positief resultaat. Zo kan hij onder meer op basis van het aantal gebruikers zelf bepalen wat de kans is op een valse identificatie. In de praktijk zal bepaald moeten worden welk kans op een fout-positief (tegen welke andere kosten) aanvaardbaar is en zal er uiteindelijk een keuze worden gemaakt.

2.4.2 Embedden

Watermerksystemen die het mogelijk maken om veel bestanden snel van een watermerk te voorzien, te kunnen detecteren en bedoeld zijn voor authenticatie en tracing zullen in de regel gebruik maken van semi dan wel blinde of publieke watermerksysteem en daarbij gebruik maken van zogeheten blind detection (par. 2.4.2). Er kunnen drie verschillende soorten algoritme voor blind embedding worden onderscheiden: hard embedding, informed embedding en informed encoding.

De meeste basisalgoritmen kunnen geclassificeerd worden als hardembedding technieken. Bij deze techniek creëert het algoritme een willekeurig patroon zonder gebruik te maken van (informatie over) het originele bestand. Dit patroon vormt het watermerk en wordt dan aan het gastobject toegevoegd.

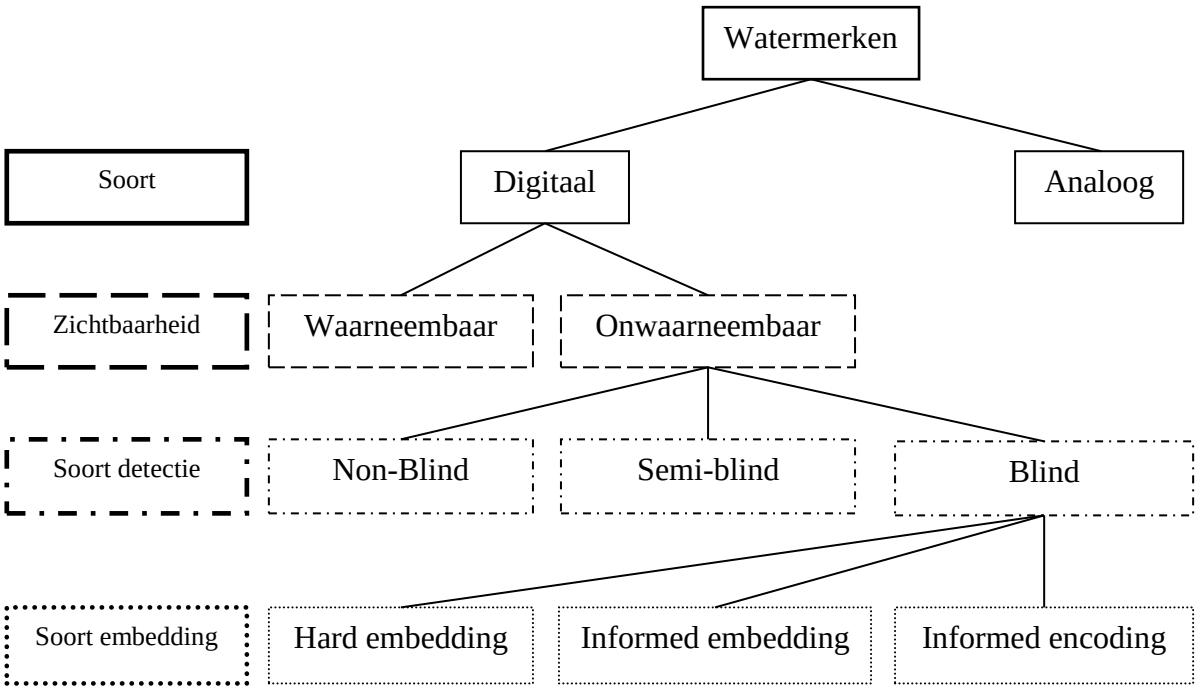
Informed embedding technieken creëren eveneens onafhankelijk van het originele bestand een patroon maar embedden dit partroon (watermerk) afhankelijk van het origineel. Bijvoorbeeld door het watermerk te plaatsen daar waar de vertekening door het embedden van het watermerk minder opvalt en daardoor sterker is.

De informed encoding technieken brengen één watermerk aan, waarbij gekozen kan worden uit een reeks watermerken waarbij je datgene kiest dat het beste "past" bij het cover work. Op

[138] Voor voorbeelden van een analytische benadering zie o.m. Cox e.a. 2008, p. 250.
[139] Cox e.a. 2007, p. 39. Zie ook par. 2.3.3.
[140] Miller, Cox & Bloom 1998, p. 75. Cox, e.a. 2007, p. 39. Ook hier bestaat een trade-off tussen de false positive rate en het aantal gemiste detecties zoals bij iedere detector het geval is. Een verlaging van de false positive rate leidt er doorgaans dan ook toe dat er een verhoging optreedt van het aantal gemiste detecties. Zie o.m. TNO 2010, p. 32.

basis van informatie over het originele bestand wordt gekozen welk watermerk het best functioneert.

Alle voorgaande technieken maken op een verschillende wijze en in verschillende fases gebruik van het origineel (coverwork). De informed embedding codes maken daarbij gebruik van het gast-object tijdens het creëeren van het watermerk. Informed encoding technieken maken gebruik van het gastobject zowel tijdens het creëeren van het watermerk als tijdens het embedden daarvan. Kennis van het gastobject is niet alleen nodig om te beoordelen of het voldoende opslagcapaciteit biedt, maar ter beoordeling van de mate van verstoring of ruis (interference or noise) die op kan treden. Het gaat hier om de capaciteit om op de meest betrouwbaar wijze informatie te transporteren door een specifiek kanaal (Channel capacity).[141] Zo kan verstoring optreden door het embedden van een watermark, maar ook door het verspreidingskanaal.[142]



Iedere embeddingstechniek kan worden toegepast op representaties van beelden, audio of video in verschillende domeinen, zoals ruimtelijk (spatial), tijd (time), frequentie (frequency) en wavelet domeinen. Verschillende transformaties maken het mogelijk om de representaties als het ware naar een ander domein te vertalen. Voor beelden wordt vaak gebruikt gemaakt van het ruimtelijke domein waar de waarde voor iedere pixel is gegeven. Deze waarden representeren de kleur van de pixel die weer in verschillende waarden kan worden weergegeven zoals RGB, YUV, etc. In het frequentiedomein worden verschillende grootheden voor verschillende frequentie componenten berekend met behulp van

[141] Deze term wordt met name gebruikt in de computerwetenschappen, electrotechniek en informatietheorie.
[142] Zie o.m. Pierre Moulin, Joseph A. O'Sullivan, Information-Theoretic Analysis of Watermarking; Koch, E. and Zhao, J., Towards Robust and Hidden Image Copyright Labeling, presented at IEEE Workshop on Nonlinear Signal and Image Processing, 1995.

verschillende relaties of transformatie(formules), zoals Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Block-based Discrete Cosine Transform (Block based DCT) en Fourier-Mellin Transform. Een ander veelgebruikt domein is het wavelet domein waar coëfficiënten van de wavelettransformatie veranderd worden in verschillende schalen, zoals Haar-transform of Daubechies wavelets. Deze wavelettransformaties bieden in beginsel goede weerstand tegen compressietechnieken.[143]

2.4.3 Waarneembaarheid

Een belangrijke eigenschap voor onzichtbare watermerken is de waarneembaarheid (perceptual transparancy or fidelity).[144] Onwaarneembare watermerken krijgen dan ook veel aandacht in de literatuur. Het embeddingsalgoritme moet het mogelijk maken om zonder noemenswaardig kwaliteitsverlies het watermerk in het gastobject aan te brengen. Het gaat hier om de vraag of er sprake is van een door mensen waarneembaar verschil tussen het origineel en het gewatermerkte object (Just Noticeable Difference; JDN).[145] In de literatuur spreekt men ook wel over de mate waarin vertekening optreedt door de inzet van watermerktechnieken. Als gevolg van de testkosten zijn modellen ontwikkeld die het menselijk oog nabootsen zoals het Human Visual System (HVS).[146]

De waarneembaarheid is van belang voor zowel de commerciële waarde als voor de kwaliteit van de bescherming van het object. Voor de commerciële waarde is het van belang dat de kwaliteit zo hoog mogelijk is.[147] De mate van de gewenste kwaliteit kan per toepassing verschillen. Zo wordt het verschil tussen het origineel en het gewatermerkte object van audio op AM-radio onwaarneembaar vanwege de lage kwaliteit van de uitzendtechnologie. Bij uitzendingen in HDTV of DVD (audio en video) is de kwaliteit veel hoger en zullen er hogere eisen moeten worden gesteld aan de waarneembaarheid.[148]

Voor de bescherming is het van belang dat het watermerk niet waarneembaar is omdat het daardoor lastiger te verwijderen is. Zelfs op het oog onwaarneembare veranderingen worden zichtbaar wanneer men het gewatermerkte object en het origineel kan vergelijken. De eindgebruiker zal in het algemeen niet beschikken over het origineel en daardoor deze vergelijking niet kunnen maken.[149] Ook hier zijn keuzes afhankelijk van de toepassing en de

[143] Het zal duidelijk zijn dat in het verslag een expert duidelijk zal moeten maken wat de waarde is van de verschillende technieken. De waarde ervan zal mede afhangen van de vraag waar het watermerk toe dient.
[144] Perceptual transparancy (Langelaar, Setywan & Lagendijk 2000, p. 21); Imperceptibility (Kutter & , Hartung 2000, p. 106); Cox, e.a. (2007 p. 36) drukken dit uit in fidelity als 'the perceptual similarity between the unwatermarked and watermarked Works at the point at which they are presented to a consumer'.
[145] Swanson, Kobayashi & Tewfik 1998, p. 1066; Langelaar, Setywan & Lagendijk 2000, p. 21; Niu e.a 2010.
[146] Meetingen worden o.m. verricht in termen van Mean Squared Error (MSE), Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR) of Structural Similarity (SSIM), mean squared error (MSE), signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), structural similarity (SSIM). Zie o.m. Delaigle, Vleeschouwer & Macq 1998; Eyadat & Vasikarla 2005; Zhu & Liu 2009
[147] Zie o.m. Carver, Yeo & Yeung 1998, p. 47.
[148] Cox e.a., p. 38
[149] Voyatzis, Nikolaides & Pitas 1998, p. 14; Carver, Yeo & Yeung 1998, p. 47.

gewenste eigenschappen. Zo kan een filmmaatschappij in zijn productieproces ervoor kiezen om in de beginfase van de productie de zichtbaarheid van watermerken in het ruwe materiaal toe te staan in ruil voor een hogere robuustheid of lagere kosten.

Voor onzichtbare watermerken is het derhalve van belang dat de veranderingen niet door mensen kunnen worden waargenomen en dat het gewatermerkte object niet kan worden vergeleken met het origineel.

2.4.4 Capaciteit

Het laadvermogen of capaciteit (payload, capacity) van een watermerk ziet op de hoeveelheid bits die nodig zijn om het watermerk zonder waarneembaar kwaliteitsverlies aan te brengen in het gast-object.[150] Het gaat met andere woorden om de hoeveelheid informatie die in het gewatermerkte bestand kan worden aangebracht. Afhankelijk van zowel het doel als het soort gastobject (audio, video, afbeeldingen) moet worden bepaald hoeveel bits nodig en wenselijk zijn.[151]

Bij veel toepassingen dient het detectiemechanisme twee functies. Ten eerste moet het duidelijk maken of er een watermerk aanwezig is in het gast-object en bij een positieve uitslag moet het ten tweede de boodschap kunnen detecteren.[152] De capaciteit van het watermerk is direct van invloed op andere eigenschappen, zoals de zichtbaarheid en robuustheid van het watermerk, maar ook op de embedding en detectie.[153] In de literatuur wordt aangenomen dat er een mate van standaardisatie gewenst zal zijn in de hoeveelheid te embedden gegevens zoals bij de International Standard Recording Code (ISRC, 12 nummers) dat bestaat uit een code voor het land, eigenaar, jaar van opname en een serienummer.[154] Daar zou het jaar van auteursrecht (© 2012), de verleende toestemming (licentievoorwaarden) en de waardering aan toe moeten worden gevoegd. Dit zou voor deze informatie neerkomen op 60 tot 70 bit aan informatie in het gast-object.[155] Langelaar, Setywan & Lagendijk wijzen daarbij tevens op de granulariteit van watermerken dat verwijst naar de hoeveelheid data dat nodig is om één eenheid informatie (watermerk) te embedden en te detecteren.[156] Centraal staat daarbij de

[150] Zie o.m. Langelaar, Setywan & Lagendijk 2000, p. 21; Cox e.a., p. 38. Bij audio ziet dit op het aantal bits dat per seconde getransporteerd wordt. Bij foto's ziet dit op het aantal bits dat in de afbeelding (host-data) en bij video op het aantal bits per veld of frame of het aantal per seconde. Watermerksystemen die N bits coderen worden N-bit watermerken genoemd.
[151] Zie voor een verdere uitwerking o.m. Langelaar, Setywan & Lagendijk 2000, p. 21; Cox e.a., p. 38 en de daar aangehaalde literatuur.
[152] Zie o.m. Kutter & Petitcolas 1999, p. 9 (online versie); Cox e.a. 2008, p. 38 Deze watermerksystemen worden ook wel aangeduid als one-bit of zero-bit watermerk(systemen) omdat er twee mogelijke uitkomsten zijn: aanwezig of afwezigheid van een watermerk. Andere systemen worden ook wel aangeduid als multiple-bit of non-zero-bit systemen.
[153] Kutter & Petitcolas 1999, p. 227; zie ook par. 2.4.1.
[154] Kutter & Petitcolas 1999, p. 227; Langelaar, Setywan & Lagendijk 2000, p. 21
[155] Fridrich and Goljan 1999; Kutter & Petitcolas 1999, p. 227; Langelaar, Setywan & Lagendijk 2000, p. 21. Zie ook Cox e.a. 2008, par. 2.3.3, p. 38 voor voorbeelden in het kader van copycontrol.
[156] Langelaar, Setywan & Lagendijk 2000, p. 21. Granulariteit ziet op de mate waarin een groter geheel wordt opgesplitst in kleinere onderdelen.Granuliteit wordt ook wel omschreven als de kleinste eenheid waarin nog

verdeling van het watermerk. Stel dat het embedden van 70 bits aan informatie wordt verspreid over één videobeeld of verspreid over bijvoorbeeld 100 videobeelden.[157] De verspreiding over 100 is niet wenselijk omdat iedereen die maar 70 videobeelden gebruikt ervoor kan zorgen dat het watermerk niet meer te detecteren of te interpreteren is. Bij digitale video's wordt in de literatuur één seconde als kleinste auteursrechtelijke entiteit gezien.[158] Het watermerk zal geëmbed moeten worden in minder dan één seconde (fragment) van de video, dat veelal samenvalt met 25 videobeelden (frame rate). De bitrate zal dan hoger worden dan 70 bits/s.

Vanwege de onvermijdelijke trade-off lijkt het voorkeur te verdienen om de boodschap te laten bestaan uit een code die weinig ruimte inneemt en door middel van een databank naar de licentienemer verwijst. De eerder genoemde traitor tracingscodes van Tardos (par. 2.3.1.) bieden op dit moment de beste code.

2.4.5 Robuustheid

Robuustheid (robustness) ziet op mogelijkheid om het watermerk te detecteren na het verwerken van het signaal.[159] Robuustheid van een watermerk ziet met andere woorden op de capaciteit van watermerken om bewuste dan wel onbewust aanvallen te overleven. Het belang van robuustheid wordt bepaald door de gewenste toepassing. Voor het aantonen van de authenticiteit van het gastobject wordt vaak gebruikt gemaakt van fragiele watermerken. Deze watermerken hebben als voornaamste kenmerk dat de robuustheid met opzet afwezig is. Iedere verandering leidt bij deze watermerken tot aantasting of verwijdering van het watermerk waardoor later kan worden aangetoond dat het niet langer authentiek is.[160]

Voor toepassingen waarbij het watermerk belangrijke informatie bevat, zoals informatie over de licentienemer is wel van belang dat het watermerk in het gast-object blijft en dus voldoende robuust is. Het moet met andere woorden met name in staat zijn om voldoende weerstand te bieden tegen bewuste aanvallen die gericht zijn op de aantasting of verwijdering van het watermerk, zoals bij een zogenaamd collusion attack. Een watermerk kan op verschillende manieren robuuster of resistenter worden gemaakt. Dit kan bijvoorbeeld door het probleem te modelleren als een communicatiekanaal, waarbij een aanval wordt gezien als een storing (distortion). Door gebruik te maken van generieke technieken uit de communicatietheorie zoals de spread spectrum kan het watermerk robuuster worden gemaakt. Zo kan de keuze voor een bepaald domein (domain) het watermerk bestand maken tegen

betrouwbaar een watermerk gedetecteerd kan worden. Bijvoorbeeld het aantal seconden audio dat je nodig hebt om een watermerk te kunnen detecteren (TNO 2010, p. 32)

[157] De hoeveelheid beelden per seconde wordt uitgedrukt in rames per second (fps) of in hertz (Hz), hiermee wordt aangegeven hoeveel in beginsel 'losse beelden' het per seconde laat zien waardoor de film een vloeiend geheel lijkt. Voor televisiebeelden neemt men vaak 25 beelden per seconden als frame rate. Voor audio geldt in beginsel hetzelfde 1 seconde fragment of verspreid over 5 seconde audio-data.

[158] Langelaar, Setywan & Lagendijk 2000, p. 21.

[159] Cox e.a. 2008, p. 41.

[160] Langelaar, Setywan & Lagendijk 2000, p. 21; Cox e.a. 2008, p. 41 en hoofdstuk 11.

bepaalde niet-malafide aanvallen, zoals rotaties. Een andere mogelijkheid is gelegen in de wijze waarin de watermerken in het bestand worden geplaatst. Deze keuze houdt altijd een bepaalde trade-off in. Zo kan om de robuustheid te verhogen ook redundantie worden toegevoegd. In de cryptografie ziet de redundantie evenals bij watermerken op de extra informatie die aan het watermerk wordt meegegeven. Door deze redundante informatie te verspreiden over het origineel wordt de robuustheid van het watermerk versterkt doordat het watermerk (de informatie) ook kan worden uitgelezen wanneer er een klein deel wordt teruggevonden of gedetecteerd. De robuustheid neemt toe naarmate er meer code/data/watermerk beschikbaar is. Die keuze houdt wel in dat er een bepaalde trade-off ontstaat: met het toevoegen van meer informatie om de robuustheid te vergroten wordt tevens de perceptuele impact verhoogt. Onderzoekers van watermerken stellen vaak dat hun watermerktechnieken robuust en veilig zijn. De vraag hoe veilig deze watermerken zijn en hoe dit kan worden gemeten is de laatste jaren duidelijker geworden.[161] De robuustheid kan tot slot ook afhangen van de keuze voor een bepaalde detectiemethode.

Ook bij de robuustheid geldt dat een volledig robuust watermerk ten koste gaat van andere eigenschappen. In het algemeen zal daarbij het uitgangspunt zijn dat het niet mogelijk moet zijn om het watermerk te veranderen of wijzigen zonder dat een noemenswaardig kwaliteitsverlies optreedt dat normaal gebruik voldoende verstoort.[162] De gewenste verstoring zal per object en toepassing verschillen. Zo kijken filmmaatschappijen ook naar kwaliteit van de piraterij voor de vraag of en in welke mate optreden gewenst is wanneer een werk zonder licentie op internet verschijnt.

De beste methode van watermerken met een tracingsdoel is die methode die robuust genoeg is om elke vervorming in het verwerkingsproces te weerstaan ongeacht of het een normale of malafide wijze van verwerking betreft. Tot op heden bestaat deze methode nog niet en zal zowel bij het ontwerp als bij de toepassing van watermerktechnieken gezocht moeten worden naar de optimale mix tussen robuustheid enerzijds en andere eisen die afdoen aan de robuustheid anderzijds, zoals de mate waarin het watermerk waarneembaar mag zijn en hoeveel informatie men aan de content wenst toe te voegen. Afhankelijk van de gewenste toepassing zullen er zowel in het ontwerp als in te gebruiken techniek keuzes gemaakt moeten worden.[163]

2.4.6 Beveiliging

Een ander belangrijk aspect van watermerken is de beveiliging (security). Deze term wordt in de literatuur op verschillende wijze gebruikt. Enerzijds wordt de term gebruikt om de capaciteit te beschrijven om aanvallen te weerstaan. Deze aanvallen kunnen onbewust of

[161] Zie Sai Ho Kwok, Watermark-Based Copyright Protection System Security, Communications of the ACM, October 2003/Vol. 46, Issue 10, p. 98-101.
[162] Craver, Yeo & Yeung 1998, p. 50; Langelaar, Setywan & Lagendijk 2000, p. 22.
[163] Voor methoden om watermerken robuust te maken en de keuzes die daarbij gemaakt kunnen worden zie o.m. Cox e.a. 2008 hoofdstuk 9.

bewust plaatsvinden. Onbewuste aanvallen zien in het algemeen op normaal gebruik van het gastobject en de signaalverwerking.[164] Zo wordt het watermerk aangevallen wanneer een gebruiker een foto verkleint of een ander bestandsformaat geeft. Het watermerk moet dus in ieder geval robuust genoeg zijn om bestand te zijn tegen normaal gebruik. Bij bewuste aanvallen is de aanvaller bewust op zoek gegaan naar methoden om het watermerk onbruikbaar te maken, bijvoorbeeld door het aan te tasten of te verwijderen. Een belangrijk deel van de literatuur bestaat uit het ontwikkelen en beschrijven van aanvallen en maatregelen daartegen (countermeasures) vanuit de gedachte dat onderzoek daarnaar bijdraagt aan de ontwikkeling van digitale watermerktechnologie.[165] Anderzijds wordt de term enger gebruikt voor een specifiek aspect van beveiliging, namelijk de geheimhouding van informatie voor ongeautoriseerde gebruikers, zoals de geheime sleutel die gebruikt wordt tijdens het embeddings- en decoderingsproces.[166] Om de kans dat de inhoud van het watermerk, bijvoorbeeld een identificatienummer, verkeerd wordt afgelezen door de detector kleiner te maken wordt de boodschap in de vorm van een watermerk vaak extra beschermd met foutverbeterende codes voordat deze in de content wordt aangebracht.[167] Daarnaast kan op een vertrouwelijke boodschap ook nog encryptie worden toegepast. Ten aanzien van de eerste omschrijving is het tevens van belang op te merken dat in de literatuur de termen 'robuustheid' en 'beveiliging' naar inhoud niet altijd eenduidig zijn.[168] Dit verschijnsel kan deels worden verklaard vanuit de historie dat de watermerkliteratuur in het begin vanuit de gedachte van kopieerbeveiliging vooral geconcentreerd was op onderzoek naar aanvallen en tegenaanvallen. De betreffende kwaliteit van watermerken werd benoemd in termen van robuustheid. Deze aanvallen werden onderscheiden in intentieloze aanvallen (non-intentional attacks) zoals bij normaal gebruik (filtering, compressie, etc) en bewuste aanvallen (intentional of malicious attacks) die gericht waren op verwijderen of aanpassen van de watermerken of gebaseerd waren op de beschikbaarheid van het embeddingsproces.[169] De aandacht voor deze laatste categorie bracht meer literatuur op gang over de beveiliging van geheime informatie. In beginsel ziet robuustheid op de mogelijkheden van watermerken om aanvallen ter overleven en de beveiliging op de mogelijkheid om de gewenste onderdelen geheim te houden. Beiden vormen een aspect van beveiliging van watermerksystemen. Minder aandacht is ervoor het brede perspectief van beveiliging die samenhangt met de wijze waarop het proces is ingericht. Dit geldt te meer wanneer het watermerk bestaat uit een code die verwijst naar een databank met licentienemers. Ook daar spelen vragen rondom beveiliging een belangrijke rol.

[164] Bij het versturen van een bestand van bijvoorbeeld een laptop naar het internet ondergaat het bestaande een aantal verwerkingen waardoor er kleine verschillen kunnen ontstaan. Ook is het denkbaar dat in bijvoorbeeld een afbeelding wordt gesneden. Het watermerk moet voldoende robuust zijn om die veel voorkomende processen en aanvallen te kunnen weerstaan.
[165] Zie o.m. Cox & Linnartz 1998, p. 7; Kutter, Voloshynovskiy & Herrigel 2000 (p. 1); Cox e.a. 2008, p. 42, p. 340. CNRS & UVIGO 2008 (Ecrypt), p. 5.
[166] Zie o.m. Langelaar, Setywan & Lagendijk 2000, p. 22; Pérez-Freire 2008, p. 9.
[167] TNO 2010, p. 32.
[168] Zie daarvoor Kalker 2001; Cayre, Fontaine & Furon 2005; Lafaye 2007 p. 462; CNRS &UVIGO 2008, p. 5.
[169] CNRS &UVIGO 2008, p. 5. Zie bijvoorbeeld Cox & Linnartz 1998.

Bij de beveiliging van watermerksystemen geldt onverkort de stelling van Kerckhoffs (par. 2.2.23) dat men er vanuit moet gaan dat de methode om de data te encrypten bekend zal zijn bij de ongeautoriseerde gebruiker en dat de beveiliging moet liggen in de gekozen sleutel. Niettemin, het hoogste niveau van geheimhouding bestaat eruit dat de ongeautoriseerde gebruiker zowel niet op de hoogte is van het feit dat er een watermerk in het bestand is opgenomen als dat hij niet beschikt over de juiste sleutel. Een niveau lager is de geheimhouding beperkt tot de sleutel, maar is de gebruiker wel op de hoogte van het feit dat er een watermerk in de content aanwezig is. Bijvoorbeeld omdat de gebruiker bij het sluiten van een overeenkomst of bij het openen van een bestand wordt gewezen op de aanwezigheid van een watermerk of de beschikking heeft gekregen over een embeddingssoftware. Een watermerksysteem kan dan als veilig worden aangemerkt wanneer kennis over zowel de gebruikte algoritmes voor embedding en extractie de ongeautoriseerde gebruiker niet helpt bij de detectie van de aanwezigheid van het watermerk als bij de verwijdering daarvan.[170]

De eisen die aan de beveiliging van watermerksystemen moet worden gesteld verschillen per applicatie en zijn afhankelijk van aannemelijke aanvallen.[171] De meeste toepassingen die zien op de bescherming van auteursrecht zullen beveiligd moeten worden tegen verschillende vormen van met name bewuste aanvallen. Welke maatregelen nodig zijn hangt dan weer af van de toepassing. Bij kopieerbeveiliging zal de aandacht gericht zijn op de beveiliging tegen ongeautoriseerde verwijdering, terwijl men bij systemen waar men het watermerk nodig heeft om te mogen kopiëren de beveiliging gericht zal zijn op het voorkomen dat een watermerk aan objecten wordt toegevoegd. De beveiliging van watermerken die gericht zijn op traitor tracing zal vooral gericht zijn op de meest aannemelijke bewuste en onbewuste aanvallen (aanpassen, verwijderen, etc.), alsmede op de geheimhouding van de sleutels. In het gehele proces zal het ook van belang zijn om aandacht te hebben voor de beveiliging van de databanken. Ook de hoogte van de beveiliging is afhankelijk van de toepassing die kan variëren van auteursrecht, patiëntendossiers tot militaire doeleinden.

2.4.7 Kosten

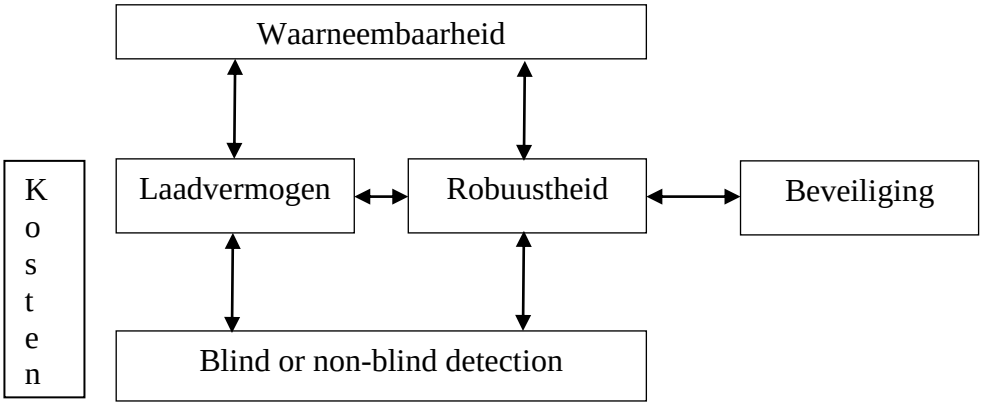
Tot slot zijn er overwegingen ten aanzien van de kosten. De kosten kunnen zowel technisch als financieel van aard zijn.[172] De financiële kosten van het ontwikkelen en operationaliseren van watermerksystemen verschillen per toepassing en businessmodel.[173] De kosten voor watermerksystemen zijn daarmee in het algemeen lastig vast te stellen. Financiële kosten spelen niet alleen een belangrijke rol bij de beslissingen of men kiest voor watermerken als een (deel)oplossing voor het handhavingsprobleem, maar ook bij de keuze tussen de verschillende eigenschappen van watermerktechnieken en bij de keuze voor een watermerksysteem. Waarbij het niet alleen de vraag is of het systeem in staat is om snel een

[170] Ruanaidh & Pereira 1998; Langelaar, Setywan & Lagendijk 2000, p. 22
[171] Zie o.m. Cox e.a. 2008, p. 335.
[172] Bij technische kosten kan gedacht worden aan computionele kosten. Dit zijn (reken)kosten die bijvoorbeeld voortkomen uit algoritmen die worden gebruikt bij het embedden en extraheren van het watermerk.
[173] Zie o.m. Decker 2001 over commercial watermarking.

watermerk in het gastobject te embedden en detecteren, maar ook hoeveel embedders en detectoren daarvoor nodig zijn.[174] De kosten spelen niet alleen een rol bij de aanschafbeslissing maar ook bij de vraag wat redelijkerwijs verwacht kan worden ten aanzien van de inzet van watermerksystemen dan wel andere DRM-systemen in termen van te verwachten opbrengsten.

2.4.8 Tussenconclusie: over keuzes en betrouwbaarheid

Er zit een zekere wisselwerking/correlatie tussen de robuustheid en beveiliging enerzijds en de zichtbaarheid en capaciteit anderzijds. Deze wisselwerking wordt duidelijk wanneer wij ons concentreren op de mogelijk malafide aanvallen op het watermerk. De eerste verdedigingslinie wordt daarbij gevormd door de onzichtbaarheid van het watermerk. Deze wordt beïnvloed door de capaciteit van de boodschap. Kort gezegd, hoe groter de boodschap, hoe beter waarneembaar het watermerk wordt en daarmee wordt direct de eerste verdedigingslinie aangetast.



Dit schema is ontleend aan Langelaar, Setywan & Lagendijk 2000

In beginsel gelden ervoor alle watermerksystemen een aantal algemene eigenschappen die van invloed zijn op de betrouwbaarheid van het specifieke watermerk.[175] De eerste eigenschap ziet op de zichtbaarheid van het systeem (par. 2.4.3). Hiermee wordt tot uitdrukking gebracht dat de vervorming (distortion) die gepaard gaan met het embedden van het watermerk niet mag leiden tot een bepaalde zichtbaarheid van het watermerk. Men spreekt daarbij ook wel van een drempel (perceptible threshold) waarmee de vervorming wordt gekwantificeerd. De mate van onzichtbaarheid heeft daarmee gevolgen voor de hoeveelheid code (of pixels) die men kan gebruiken bij het embedden van een watermerk. Kort gezegd, de hoeveelheid informatie (code) is direct van invloed op de zichtbaarheid van het watermerk. Een tweede eigenschap wordt gevormd door de robuustheid. Deze kan bijvoorbeeld worden vergroot door het toevoegen van redundantie (par. 2.4.5). Hierdoor wordt de robuustheid van het watermerk

[174] Cox e.a. 2008, par. 2.3.10, p. 46.
[175] Deze eigenschappen vindt men veelal ook terug in de cryptografie en gelden voor zowel audio, video als afbeeldingen.

versterkt. Die keuze houdt wel in dat er een bepaalde trade-off ontstaat: met het toevoegen van meer informatie om de robuustheid te vergroten wordt tevens de perceptuele impact verhoogt. Daarnaast geldt er een trade-off tussen de robuustheid en de lengte van de code (payload).[176]

Het is in veel gevallen mogelijk om meerdere watermerken in een object aan te brengen. De combinatie van meerdere watermerken is en wordt niet nader besproken. Maar duidelijk zal zijn dat ook dit van invloed is op de eigenschappen van de verschillende watermerken. Het is van belang de trade-off op waarde te schatten. De trade-off mag niet worden gezien als een argument om het watermerk altijd als een zwakke techniek neer te zetten. De trade-off is evenals bij andere technieken onvermijdelijk. De keuze van eigenschappen in relatie tot de toepassing kan wel een indicatie vormen voor de betrouwbaarheid van het watermerk. Zo kunnen ongelukkige keuzes van de eigenschappen van het watermerk en de toepassing een indicatie vormen van meer fouten in het proces. Voor het gebruik van bewijs is het van belang dat deze keuzes inzichtelijk worden gemaakt en worden verantwoord in relatie tot de betrouwbaarheid.

2.5 Meest aannemelijke aanvallen

Naast verkeerde keuzes bij de inzet van verschillende eigenschappen in relatie tot het doel van het watermerk kunnen zogenoemde aanvallen de betrouwbaarheid van watermerken aantasten. Deze aanvallen kunnen worden gedefinieerd als ieder proces dat bedoeld is om het doel van het watermerk teniet te doen.[177] Een veilige watermerktechniek is dan een techniek waarbij het voor aanvallers niet mogelijk is om het watermerk te veranderen of te verwijderen. In de literatuur wordt bij de presentatie van nieuwe systemen of technieken in relatie tot de betrouwbaarheid van het systeem dan ook altijd aandacht besteed aan de mate waarin de techniek bestand is tegen de meest aannemelijke aanvallen. Men concentreert zich in de literatuur op de meest aannemelijke aanvallen omdat niet elke aanval relevant is voor elk systeem.[178] Kennis van watermerken is daarbij van groot belang, omdat getaxeerd zal moeten worden of het beroep van een gedaagde op een bepaalde aanval in het licht van het gebruikte watermerksysteem de betrouwbaarheid ervan aantast.

In de literatuur worden aanvallen op verschillende wijzen benaderd. Hieronder worden er drie besproken. Zo onderscheiden sommigen de aanvallen op basis van het effect dat zij hebben op het watermerk of het gebruik van de resultaten daarvan.[179] De hier besproken indelingen zijn bedoeld om een beter zicht te krijgen op de mogelijk aanvallen en beperkingen van watermerksystemen. Hierbij moet worden opgemerkt dat dit domein continue in ontwikkeling is. De toename van watermerksystemen zal ook leiden tot meer soorten aanvallen waardoor de

[176] De payload bepaalt hoeveel code er in moet en de capaciteit hoeveel code er in kan.
[177] Zie o.m. Cox. e.a. 2007, par. 2.3, p. 41.
[178] Men zet zichzelf als het ware in de hackermodus. ‘Wat zou ik doen als ik mijn systeem zou aanvallen’.
[179] Cox & Linnartz 1998; Craver e.a. 1998, p. 51; Nikolaidis e.a. 2001, p. 1-2. Anders Petitcolas, Anderson & Kuhn 1999, p. 1069.

gekozen categorieën in de toekomst veel meer aanvallen kunnen en zullen herbergen dan hier is aangegeven. Daarnaast is het ook mogelijk dat een aanvaller meerdere of een combinatie van aanvallen tegelijk inzet.[180]

2.5.1 Life-cycle benadering van Carver e.a.

Carver, Yeo en Yeung benaderen de aanvallen vanuit de life-cycle van aanbrengen, distribueren, detecteren en interpreteren. Zij onderscheiden daar vier soorten aanvallen.[181]

Ten eerste aanvallen die de robuustheid van het watermark aanvallen (Robustness attacks) die erop gericht zijn om watermerken te verbergen of te verwijderen. Bekende aanvallen in deze categorie zijn aanvallen met behulp van jitter (Jitter attack) waardoor kwaliteitsverlies optreedt bij geluiden.[182] Of StirMark-aanvallen die gebruik maken van algemene tools die in staat zijn een verstoring of een combinatie van verstoringen te bewerkstelligen met als doel om detectie te voorkomen zonder dat de waarneembaarheid van het gastobject vermindert.[183]

Ten tweede aanvallen die gericht zijn op de representatie van de content, bijvoorbeeld roteren van een afbeelding, zodat het detectiemechanisme afhankelijk van het gekozen transformatie domein het watermerk niet meer kan detecteren (presentation attacks). Tot deze categorie hoort ook de zogenoemde Mozaïek aanval (Mosaic attack) die het mogelijk maakt het watermerk uit een afbeelding te verwijderen.[184] Maar ook vaak onbewuste aanvallen, zoals rotatie kunnen het in beginsel mogelijk maken dat het watermerk niet langer in het gastobject kan worden gevonden.

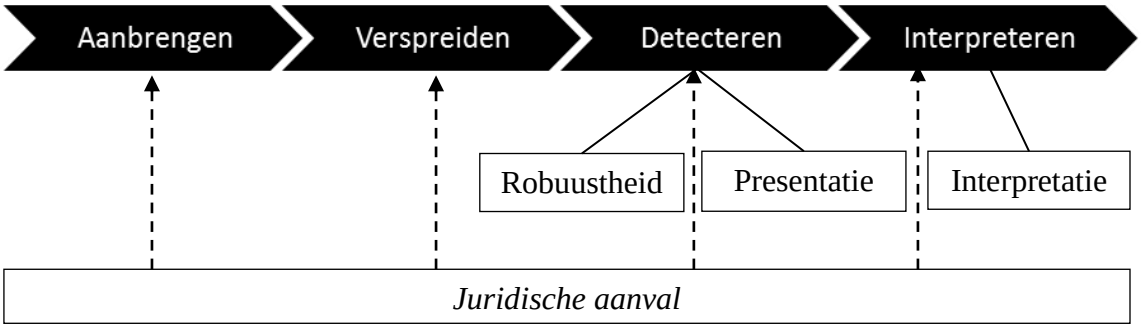
Ten derde aanvallen die de interpretatie van watermerken onmogelijk maken (interpretation (protocol) attacks), bijvoorbeeld bij authenticatie. Deze aanval heeft als doel het watermerksysteem als onbetrouwbaar aan te kunnen duiden. Zo kan er, wanneer er niet van een TTP gebruik wordt gemaakt een probleem ontstaan wanneer de aanvaller zelf een eigen watermerk aanbrengt (dead-lockstrategy).[185] Door een eigen watermerk in de content aan te brengen kan het lastig zijn te bepalen wie nu de eigenaar is van de content. Na vergelijking zal blijken dat dit niet mogelijk is waardoor het systeem als onbetrouwbaar wordt aangezien.

Ten vierde de laatste categorie is de zogenoemde juridische aanval die niet langer op technische gronden maar op juridische gronden het watermerk als bewijs aanvalt. In deze groep worden alle niet-technische aanvallen geplaatst die de geloofwaardigheid van het watermerk als bewijsmiddel aantasten. Daarbij kan gedacht worden aan wetgeving die bijvoorbeeld de inzet of de betrouwbaarheid van watermerken reguleert, maar ook aan het

[180] Kutter, Voloshynovskiy & Herrigel 2000 (p. 3).
[181] Carver, Yeo & Yeung 1998.
[182] Zie o.m. Petitcolas, Anderson & Kuhn 1998, p. 223. Jitter verwijst naar de onregelmatigheid in de tijdbasis van een digitaal signaal of het hierdoor veroorzaakte storende signaal, waardoor kwaliteitsverlies optreedt bij geluiden. Een methode om dat te voorkomen is echo hiding.
[183] Zie o.m. Petitcolas, Anderson & Kuhn 1998, p. 224;
[184] Zie uitgebreid o.m. Petitcolas, Anderson & Kuhn 1998, p. 228. Dit is bijvoorbeeld mogelijk door een afbeelding op te delen in verschillende delen en later weer in elkaar te zetten. Een eenvoudig detectiemechnisme zal hierdoor niet in staat zijn het watermerk te vinden.
[185] Kwok 2003. In dit geval kan zich ook het probleem voor doen dat men het watermerk van een ander niet kan detecteren omdat ieder zijn eigen detectiemechnisme gebruikt. In de praktijk zal men elkaar hier op wijzen.

aantasten van de geloofwaardigheid van de TTP, de deskundige of toelaatbaarheid van het watermerk als bewijsmiddel. Ten aanzien van de authenticatie van content merken Cox e.a. op dat bij veel toepassingen de toegestane verstoringen niet slechts een technische, maar ook vooral een juridische kant hebben. De verdeling tussen verstoringen die de rechtbank zal toestaan en verstoringen die zij niet zullen toestaan is volgens hen dan ook een kwestie van jurisprudentie. Zij wijzen erop dat uitspraken over deze verstoringen lastig te voorspellen zijn omdat deze ook afhankelijk zijn van de vaardigheden van advocaten en de technische merites van het argument dat zij in een eerste zaak naar voren kunnen brengen. Deze gerechtelijke uitspraken kunnen volgens hen dan ook leiden tot verrassende tegenstrijdigheden. Zij noemen daarbij het voorbeeld dat sommige verstoringen (distortions) toegestaan kunnen worden wanneer de verwerking plaats heeft gehad in het ruimtelijk (spatial) of tijd (temporal) domein, maar niet wanneer deze heeft plaatsgevonden in het frequentie (frequency) domein, ook niet in die gevallen waarin de verwerking lineair is en de resultaten gelijk zijn. Tevens wijzen zij op de verschillen die kunnen ontstaan in de verschillende jurisdicties en dat de toegestane verstoringen in de tijd kunnen veranderen.

In de kern richt iedere aanval zich afhankelijk van de toepassing op een onderdeel van het watermerksysteem.[186] Een juridische aanval onderscheidt zich van de technische aanval omdat er naast vragen over de waardering van het watermerk ook een aanval kan worden ingezet op het gehele systeem, zoals vragen over de toelaatbaarheid of relevantie van watermerken als bewijs.



Aanvallen van het proces

Petitcolas, Anderson & Kuhn merken op dat de verschillen tussen de categorieën niet altijd helder zijn omdat bepaalde aanvallen zoals een StirMark aanval zowel gericht zijn op het maskeren van het watermerk als op het verstoren van de content om het detectiemechnisme te misleiden.[187] Zij doen ook geen andere voorstellen maar richten zich evenals de meeste anderen verder op de bespreking van bepaalde aanvallen. Wel wijzen zij in termen van beperkingen op twee andere invloeden: de omgeving waarin het watermerk moet functioneren en de implementatie van watermerksystemen.[188] Een ander in de literatuur veel gemaakt

[186] Er kan ook gedacht worden aan een aanval op het systeem door bijvoorbeeld bij kopieerbeveiliging het detectiemechanisme fysiek te verwijderen. Deze toepassing van watermerken blijft echter buiten beschouwing.
[187] Petitcolas, Anderson & Kuhn 1999, p. 1069.
[188] Petitcolas, Anderson & Kuhn 1999, p. 1071.

onderscheid is tussen zogenoemde signaaltransformaties en bewuste (intentional) aanvallen.[189] In veel gevallen gaat men er daarbij vanuit dat signaal transformaties onbewust (unintentional) plaatsvinden, bijvoorbeeld door het croppen of comprimeren van een afbeelding. Bewuste aanvallen gaan verder omdat de aanvaller zijn kennis wil gebruiken om het watermerk bewust aan te tasten of te verwijderen. Cox e.a. komen tot drie categorieën aanvallen, het ongeautoriseerd aantasten, embedden en detecteren.[190]

2.5.2 Voorkomen van detectie of vervals-benadering van Cox e.a.

Cox e.a. geven een andere indeling van de aanvallen. Het belang van iedere aanval is afhankelijk van de toepassing. In tegenstelling tot watermerken die gericht zijn op het beschermen van content zullen bijvoorbeeld watermerken die meer functionaliteiten bieden aan consumenten in de regel nauwelijks bloot staan aan bewuste aanvallen.

De eerste categorie ziet op het aantasten van het watermerk met als doel te voorkomen dat het watermerk gedetecteerd wordt.[191] Het succes van deze aanval hangt samen met het gebruikte domein (domain) en detectiemethode. Binnen deze categorie kan een onderscheid worden gemaakt tussen aanvallen die bedoeld zijn om het watermerk te elimineren en het watermerk te maskeren.[192] Het verschil tussen beiden is gelegen in de vraag of het watermerk is verdwenen of niet. Watermerken zijn geëlimineerd als het watermerk is verwijderd uit het gastobject, terwijl het watermerk verborgen is wanneer het slechts met niet gebruikelijke en dus zeer geavanceerde detectiemechanisme weer kan worden teruggevonden. Zo zijn veel watermerkdetectiemechanismen niet in staat watermerken te detecteren van afbeeldingen die licht geroteerd zijn. Hiermee is het watermerk voor het detectiemechnisme verdwenen, terwijl in werkelijkheid een systeem dat in staat is een correctie toe te passen voor de rotatie het watermerk wel kan vinden.

Een veel besproken aanval in deze categorie is de zogenoemde collusie aanval (collusion attack).[193] Het succes van een collusion attack hangt mede af van de gebruikte watermerk boodschap. Bij deze aanval heeft een aanvaller of groep het bezit gekregen over een aantal objecten die ieder voorzien zijn van een uniek watermerk. Vervolgens zullen zij proberen met al deze versies inzicht te krijgen in welke methode is gebruikt om uiteindelijk een object te krijgen zonder watermerk. In de praktijk zal het niet heel moeilijk zijn verschillende objecten te verkrijgen.[194] Doordat watermerken in beginsel worden gevormd door veranderingen (zie

[189] Zie o.m. Cox & Linnartz 1998. Signaal transformaties zien op de wijze waarop een signaal wordt overgebracht en in deze zin op de wijze waarop dat signaal kan worden verstoord. Bijvoorbeeld door compressie of door data dat niet gebruikt wordt voor het transporteren van een signaal maar enkel geproduceerd wordt als bijproduct van andere activiteiten, vaak aangeduid als Noise en in relatie tussen bruikbare en irrelevantie informatie in een signaal uitgedrukt ‘Signal-to-noise ratio’.
[190] Zie voor verschillende indelingen o.m. Carver, Yeo & Yeung 1998, p. 46; Cox & Linnartz 1998, p. 7 (OL); Petitcolas, Anderson & Kuhn 1999, p. 1069; Cox e.a. 2008, p. 42, p. 340.
[191] Cox e.a. 2008, p. 42, p. 340. duiden deze categorie als unauthorized removal.
[192] Cox e.a. 2008, p. 342.
[193] Zie o.m. Petitcolas, Anderson & Kuhn 1999, p. 1069.
[194] Zie bijvoorbeeld Hoffelder die in zijn weblog over het gekraakte en gewatermerkte e-book van Harry Potter een collusie aanval beschrijft: ‘I’m pretty sure the file names are also used as a digital watermark. I just got my

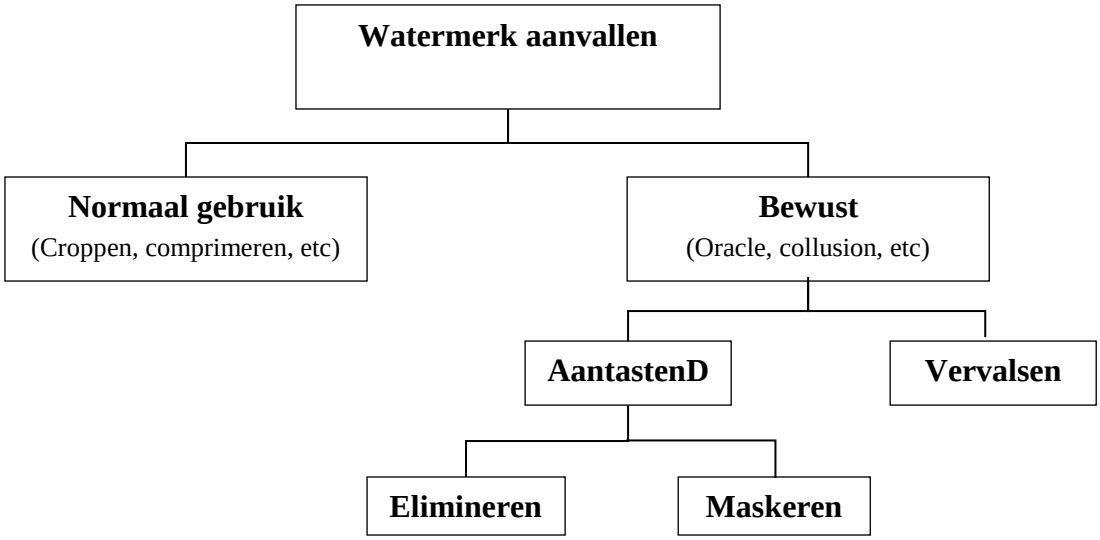
par. 2.2.3) kan de aanvaller vervolgens de verschillende versies met elkaar vergelijken en op die wijze de veranderingen blootleggen en het watermerk beetje bij beetje verwijderen. Naarmate de aanvaller meer kopieën tot zijn beschikking heeft zal hij beter in staat zijn het watermerk aan te tasten zonder de kwaliteit van het gastobject aan te tasten. In het algemeen wordt aangenomen dat een beperkt/klein aantal kopieën voldoende is voor een succesvolle aanval.[195] Uiteindelijk zal hij op deze manier in staat zijn een origineel te reproduceren zonder watermerk. Deze aanval is vroeg onderkend en heeft inmiddels ook geleid tot diverse oplossingen of tegenmaatregelen in verschillende systemen. Voor traitor tracingsdoeleinden worden de codes van Tardos als beste gezien. Zij kunnen collusion attacks overleven en toch met grote zekerheid achterhalen wie met wie samenwerkte. Daarnaast bieden zij een heel kleine kans dat een onschuldige wordt aangeduid. Een collusie aanval blijft altijd mogelijk. In de praktijk is gewatermerkte content in beginsel van hoogwaardige kwaliteit waardoor er voldoende ruimte is om meerdere watermerken aan te brengen en te verbergen. Daarbij komt dat een aanvaller die geen toegang heeft tot een niet-gewatermerkt origineel nooit zeker zal weten of hij alle watermerken heeft verwijderd. Ook bij deze aanval speelt de toepassing een rol. Zo zal het eenvoudiger zijn een paar kopieën te verkrijgen van een film die door iedereen kan worden aangeschaft dan in een situatie waarin de film zich nog in de productiefase bevindt omdat het aantal mensen dat die film ter beschikking heeft veel kleiner is.

De tweede categorie herbergt alle watermerkaanvallen die in staat zijn om watermerken te vervalsen.[196] In tegenstelling tot de vorige categorie aanvallen kan het watermerk wel eenvoudig worden gedetecteerd maar is het de vraag of het juiste watermerk gedetecteerd is (vals positief). Wanneer aangetoond kan worden dat het betreffende watermerksysteem hier gevoelig voor is dan ligt het in de lijn der verwachting om vervolgens de stelling te betrekken dat niet zeker is of het watermerk wel afkomstig is van gedaagde dan wel verdachte. Dit is mogelijk doordat een aanvaller er een eigen watermerk aan heeft toegevoegd of door een watermerk van iemand anders in een nieuw gastobject te plaatsen.

hands on a second copy of HP1 and the internal files have different names. http://www.the-digital-reader.com/2012/03/28/pottermore-drm-is-hacked-provided-by-booxstream/#.T9XQE8Uwz90

[195] Cox e.a. 2008, p. 42.

[196] Cox e.a. 2008, p. 43 noemt deze categorie embedding en refereert naar vervalsing (forgery).

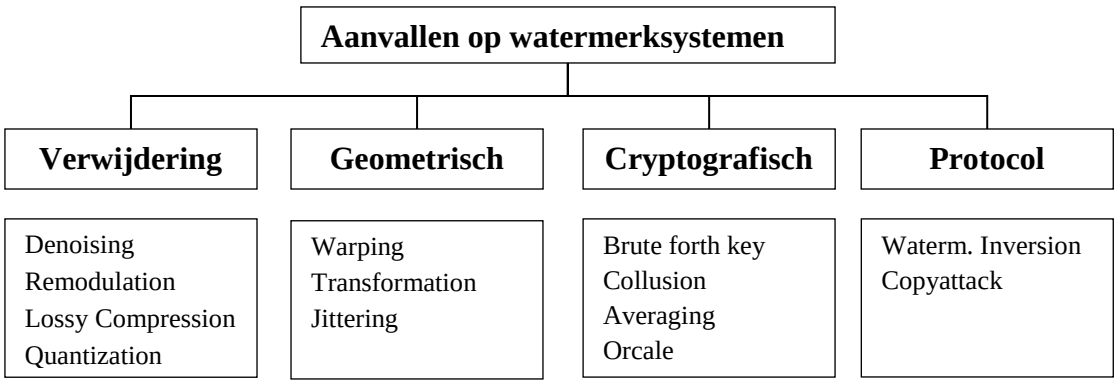


Categorieën van aanvallen van watermerken

2.5.3 De type-indeling van Kutter e.a.

Tot slot Kutter, Voloshynovskiy & Herrigel categoriseren de malafide of bewuste aanvallen naar vier categorieen: removal attacks, geometrical attacks, cryptographic attacks en protocol attacks.[197] De removal attacks richten zich evenals bij de anderen op het verwijderen van het watermerk met als doel de inhoud onleesbaar of de detectie onmogelijk te maken. De geometrical attacks hebben niet tot doel het watermerk te verwijderen maar om een zodanige verstoring tot stand te brengen dat het detectiemechanisme niet langer in staat is het watermerk te vinden dan wel uit te lezen.[198] Cryptographic attacks zijn aanvallen die veelal afkomstig zijn uit de cryptografie maar een bijzondere waarde krijgen bij watermerken. Een voorbeeld hiervan zijn de aanvallen waarbij gebruik wordt gemaakt van brute rekenkracht (brute force attacks) om de geheime informatie te ontsleutelen.[199] Men probeert met andere woorden de sleutel met grof rekengeweld te verkrijgen. Andere aanvallen in deze categorie zijn de zogenoemde protocol attacks, statistical averaging en collusion attacks. De protocol attack richt zich op het concept van het gekozen watermerksysteem en niet op de verwijdering van het watermerk of het uitschakelen van de detectie. Een voorbeeld hiervan is het zogenoemde copy attack, waarbij men gebruikt maakt van het concept van het watermerksysteem dat er vanuit gaat dat het niet mogelijk moet zijn het watermerk door een vergelijking met een niet-gewatermerkt gastobject te verkrijgen.

[197] Kutter, Voloshynovskiy & Herrigel 2000.
[198] Door veranderingen (in ruimte of tijd) aan te brengen ten aanzien van de verborgen (stego) data. Dit kan bijvoorbeeld door een afbeelding of film te schalen. Denk hierbij aan het uitprinten van een foto en het opnieuw inscannen daarvan of aan het iets scheef houden van een camera bij het opnemen van een film in de bioscoop. Het watermerk zit vaak nog wel in het bestand maar de detectie zal in deze gevallen veel lastiger zijn omdat de exacte locatie van de boodschap (watermerk) gewijzigd is en een (blinde) detector derhalve niet bekend is. Ook hier zijn weer oplossingen voor. Zie voor eenvoudige voorbeelden o.m. TNO 2011, p. 35.
[199] Op basis van de wet van Kerckshoff kan men er vanuit gaan dat het algoritme al bekend is.



Dit schema is ontleend aan Kutter, Voloshynovskiy & Herrigel 2000

Voor watermerken die traitor tracing als hoofddoel hebben is het van belang dat deze niet verwijderd kunnen worden zonder dat er noemenswaardig kwaliteitsverlies optreedt. Watermerken moeten met andere woorden voldoende robuust zijn om verwijdering tegen te gaan dan wel voldoende kwaliteitsverlies opleveren dat het bestand nagenoeg onbruikbaar wordt wanneer het watermerk wordt aangetast of verwijderd.

2.6 Samenvatting en conclusie

Digitaal watermerken is kort gezegd een techniek om een boodschap te embedden in een digitaal signaal of gastobject. Het vormt daarmee de digitale variant van het analoge watermerk waarvan het watermerk in het bankbiljet het bekendste voorbeeld is.

De techniek van digitaal watermerken wordt eind jaren tachtig geïntroduceerd en komt halverwege de jaren negentig in de belangstelling te staan van onder meer de EU en de industrie vanwege de potentiële toepassingen voor het handhaven van intellectuele rechten in een digitale omgeving. Dit resulteert in een ontwikkeling van theoretische modellen die met name na de eeuwwisseling steeds meer volwassen worden en steeds vaker worden ingezet.

Watermerken worden in de literatuur op een aantal wijzen geclassificeerd. Ten eerste wordt er een onderscheid gemaakt tussen analoge (bankbiljet) en digitale watermerk-technieken. Bij digitale watermerken wordt daarna een onderscheid gemaakt tussen waarneembare en onwaarneembare watermerken waarbij bij beeldmateriaal ook wel wordt gesproken over zichtbare en onzichtbare watermerken.

Bij het ontwikkelen van onwaarneembare watermerken wordt gebruik gemaakt van verschillende technieken en principes uit de cryptografie en steganografie. Om watermerken onwaarneembaar te embedden wordt met behulp van verschillende technieken gebruikt gemaakt van de binaire code (nullen en enen) van het gastobject. Zo is een foto opgebouwd uit verschillende pixels waarbij iedere pixel een eigen binaire code heeft. Bij een methode zoals de Least Significant Bit modification (LSB) gaat men op zoek naar een deel van de foto waar het niet opvalt dat een pixel van kleur verschilt. Zo zal het niet opvallen wanneer je uit een foto waarop een dansend meisje met zwart haar is afgebeeld, één zwarte pixel een gradatie lichter maakt. Dat is met het blote oog onwaarneembaar en zal in beginsel alleen

opvallen wanneer je in staat bent deze foto met het origineel te vergelijken. Alleen dan wordt duidelijk waar de verschillen zitten. Deze verschillen samen vormen het watermerk. Het watermerk kan allerlei boodschappen bevatten waaronder de naam van de licentienemer. De toegepaste techniek is mede afhankelijk van het soort (audio, video, foto) en type (bestandsformaat) gastobject. Duidelijk mag zijn dat hoe meer binaire code een bestand bevat hoe eenvoudiger het in de regel is om onwaarneembare watermerken aan te brengen.

De boodschappen kunnen verschillend van aard zijn. Watermerken kunnen dan ook voor verschillende toepassingen worden ingezet, zoals voor het indexeren van reclameboodschappen voor televisie-uitzending of voor medische toepassingen in het kader van patiëntveiligheid. De meeste toepassingen dienen er de bescherming van het auteursrecht en worden in de regel benoemd aan de hand van vier doelen: identificatie van de maker, traitor tracing, authenticatie van content en regulering van content waarvan de technieken die kopieerbeveiliging mogelijk maken de bekendste is. De gewenste toepassing is van invloed op het gebruik en succes van het watermerk. Watermerken hebben verschillende eigenschappen waarbij onderling sprake is van een bepaalde trade-off, waardoor de optimale mix van eigenschappen bepaald zal moeten worden aan de hand van de toepassing van watermerken. Die afweging heeft daarmee een belangrijke invloed op het succes van watermerksystemen.

In dit onderzoek staat het onzichtbare digitale watermerk ter handhaving van het auteursrecht centraal. Meer in het bijzonder het traceren van de licentienemer, ook wel bekend als ‘(traitor) tracing’. Het idee achter deze toepassing is de rechthebbende in staat te stellen de licentienemer en daarmee de dader (traitor) te achterhalen. Deze watermerken worden in de literatuur in het domein van forensisch digitaal bewijs geplaatst. Het is van belang om op te merken dat men in de watermerkliteratuur zich vooral richt op de techniek van het watermerken en de gegevens die in het watermerk worden opgenomen als een vaststaand feit beschouwd waardoor er vanuit de watermerkliteratuur geen aandacht is voor de vraag of deze gegevens correct zijn. Voor het watermerk als bewijsmiddel is zowel de betrouwbaarheid van de gegevens die in het watermerk worden gestopt als de betrouwbaarheid van het watermerk als techniek relevant. In het vervolg van het onderzoek zal de juiste invoer van gegevens verder als uitgangspunt worden genomen, tenzij anders is beschreven. Dat betekent dat er van wordt uitgegaan dat de juiste gegevens van de licentienemer in het watermerk zijn opgenomen en dat het watermerk op de juiste wijze in het bestand is verwerkt. Wanneer een bestand op internet is aangetroffen kan het watermerk worden uitgelezen en wordt duidelijk wie de licentienemer is. Met het watermerk kan de rechthebbende aldus een verband te leggen tussen het op internet aangetroffen bestand en de licentienemer.

Bij het vaststellen van de (persoons)gegevens van de licentienemer in het kader van traitor tracing, komt het uiteindelijk neer op de vraag of het watermerk ten onrechte niemand kan vinden (fout-negatief) en of het watermerk mogelijk ten onrechte een onschuldige aanwijst (fout-positief).

Het proces van watermerken kan in vier fasen worden onderverdeeld: het aanbrengen (embedden), verspreiden, detecteren en interpreteren van een watermerk. Tijdens de eerste fase wordt informatie (het watermerk) aan het gastobject toegevoegd door middel van een sleutel en een codeeralgortime. Nadat het gewatermerkte gastobject in de tweede fase is verspreid bijvoorbeeld via het internet kan het in de derde fase worden gedetecteerd en gedecodeerd. Hiervoor is het noodzakelijk dat het gastobject zelf eerst wordt gevonden waarna het watermerk eerst moet worden gedetecteerd en daarna worden gedecodeerd. In de laatste en vierde fase moet het watermerk worden geïnterpreteerd. Dat betekent bij watermerken die voor traceerdoeleinden worden ingezet dat de boodschap moet worden gelezen en geïnterpreteerd. De resultaten leveren een kansberekening op ten aanzien van de aanwezigheid van een bepaald watermerk en uiteindelijk een kansberekening dat gevonden content toebehoort aan een bepaalde licentienemer. Dit kan ook plaatsvinden doordat er meerdere watermerken in content worden geplaatst.

Watermerktechnieken maken gebruik van een aantal eigenschappen die afhankelijk van de toepassing meer of minder gewenst zijn: waarneembaarheid, capaciteit, robuustheid, beveiliging en de kosten. Daarnaast is ook het gekozen embed- en detectiemechanisme van invloed op de betrouwbaarheid van een watermerksysteem. In bijna alle gevallen is er sprake van een trade-off en zullen er keuzes moeten worden gemaakt. Hoe groter de boodschap is die men wil verbergen hoe lastiger het zal worden om dit onwaarneembaar te doen. Om het watermerk als bewijsmiddel te kunnen gebruiken zal duidelijk moeten worden in hoeverre deze wisselwerking de betrouwbaarheid van het watermerk heeft beïnvloed.

Naast de eigen keuze voor de toepassing van watermerken en de gebruikte eigenschappen kan de betrouwbaarheid ook door zogenoemde aanvallen worden aangetast. Daarbij wordt een onderscheid gemaakt tussen aanvallen door normaal gebruik en zogenoemde malafide aanvallen waarbij in dit laatste geval de aanval opzettelijk gericht is op het onbruikbaar maken van het watermerk waardoor de betrouwbaarheid in het geding komt. Hoewel in beginsel ontelbare aanvallen denkbaar zijn wordt in de literatuur vooral gewezen op de meest aannemelijke aanvallen die bij het gepresenteerde watermerk denkbaar zijn. Vanuit de wetenschap zijn verschillende watermerksystemen gepresenteerd en becommentarieerd. Een literatuuronderzoek kan om die reden een belangrijk middel zijn om de betrouwbaarheid te onderzoeken. Ook het ‘overleven’ van competities met als doel watermerken te kraken kan een indicatie zijn van de betrouwbaarheid van het watermerksysteem. Voor het watermerk als bewijs zal het uiteindelijk van belang zijn dat duidelijk wordt hoe aannemelijk het is dat bepaalde aanvallen, de betrouwbaarheid van het watermerk en de resultaten van het proces hebben beïnvloed.
Het succes van watermerken als bewijsmiddel is afhankelijk van een juiste authenticatie van de licentienemer en de juiste toepassing van watermerktechnieken.

In dit hoofdstuk is duidelijk geworden hoe de rechthebbende met watermerken de licentienemer zou kunnen traceren wanneer deze de gewatermerkte content op internet plaatst.

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te kunnen beoordelen is het van belang om vast te stellen wat het watermerk juridisch kan bewijzen. In de context van de waarheidsvinding en mogelijke verweren is het van belang te bepalen in welke situatie het watermerk de verkeerde uitkomst kan geven.

Daarop vooruitlopend zal in hoofdstuk drie blijken dat een betrouwbaar watermerk juridisch niet meer aan het bewijs kan bijdragen dan een verband te leggen tussen het aangetroffen bestand en de licentienemer. Zo kan het watermerk geen bewijs leveren voor de stelling dat de licentienemer inbreuk op het auteursrecht van de rechthebbende heeft gepleegd. De waarde van het watermerk als bewijsmiddel blijft in die zin dus beperkt tot het leggen van een verband tussen het op internet aangetroffen bestand en de licentienemer.

Om dat verband te kunnen leggen zal kort gezegd in het gehele proces de juiste gegevens moeten zijn verkregen van de licentienemer, deze gegevens op een juiste wijze als boodschap in het watermerk zijn opgenomen en moet het watermerk deze gegevens weer juist detecteren. Daarmee is tevens gegeven welke situaties ertoe kunnen leiden dat het watermerk uiteindelijk een verkeerde uitkomst geeft. Ten aanzien van het watermerk als bewijsmiddel kan de gedaagde of verdachte in een juridische procedure dan ook twee type verweren voeren. Ten eerste kan hij wijzen op mogelijke fouten die zijn gemaakt in de authenticatieprocedure, zoals fouten in de administratie. Ten tweede kan hij erop wijzen dat er iets is fout gegaan bij het inzetten van de techniek van watermerken waardoor er sprake is van een fout-positief. Ten derde kan hij erop wijzen dat iemand anders het watermerk met zijn gegevens in de content heeft geplaatst, bijvoorbeeld bij een hack van het watermerk. In de eerste tweede gevallen kan de fout per ongeluk of met opzet hebben plaatsgevonden. Het is immers ook denkbaar dat de rechthebbende opzettelijk de gegevens of het watermerk zelf heeft gemanipuleerd.

Deze mogelijke verweren worden in hoofdstuk vier nader besproken in hun juridische context.

3 Watermerken en handhaving van het auteursrecht

‘You can get more with a kind word and a gun than you can with a kind word alone.’[1]

3.1 Inleiding

In het vorige hoofdstuk is het watermerk benaderd vanuit de techniek, waarbij de gedachte in de watermerkliteratuur steeds is geweest dat het watermerk als bewijsmiddel een bijdrage kan leveren aan de handhaving van het auteursrecht door het mogelijk te maken de vermeende licentienemer te traceren (hierna: licentienemer).[2] Vanuit die gedachte staat in dit onderzoek steeds de vraag centraal of het watermerk als juridisch bewijsmiddel kan dienen om een verband te leggen tussen het op internet aangetroffen bestand en de licentienemer.[3]

Om als juridisch bewijsmiddel bij te kunnen dragen aan de handhaving van het auteursrecht dient eerst onderzocht te worden of het watermerk geaccepteerd zal worden door de afnemers van digitale content (par. 3.2) en of het watermerk past in het handhavingsbeleid van de overheid en rechthebbenden (par. 3.3). De effectiviteit van het watermerk als juridisch bewijsmiddel wordt vooral bepaald door de rol die het krijgt in de context van het bewijsrecht. Om te kunnen bepalen welke rol het watermerk kan spelen bij het vaststellen van inbreuk op het auteursrecht is nagegaan wanneer er sprake is van inbreuk op het auteursrecht. (par. 3.4). Tot slot is er aandacht voor de juridische bescherming van watermerken tegen verwijdering uit de digitale content (3.5).

In de navolgende paragraaf wordt eerst de mogelijke rol van het watermerk onderzocht bij de handhaving van het auteursrecht vanuit het perspectief van consumenten en uploaders (par. 3.2). Daarbij wordt in het licht van Digital Rights Management (DRM) en de kopieerbeveiliging in het bijzonder, eerst gekeken naar de vraag of consumenten bereid zijn het watermerk als bewijsmiddel te accepteren. Daarna wordt gekeken naar de vraag of het watermerk aansluiting vindt bij de drijfveren van consumenten om content te kopen en weerstand biedt tegen de drijfveren van uploaders en verspreiders van content om deze te verspreiden. Vervolgens wordt aandacht besteed aan de vraag of het watermerk aansluit bij het handhavingsbeleid van zowel de overheid als particulieren (par. 3.3). Voor watermerken is het voorts van belang te kijken naar de vraag welke rol het watermerk kan spelen bij het bewijzen van inbreuk op het auteursrecht (par. 3.4). Centraal staat daarbij de vraag wat bewezen moet worden om inbreuk op het auteursrecht vast te stellen (probandum) en welke rol het watermerk daarbij als bewijsmiddel kan spelen. Als voorwaarde om als bewijs te kunnen dienen mag het watermerk niet uit de gastobjecten verwijderd zijn. De wijze waarop

[1] Toegeschreven aan Al Capone (1899-1947). De bron is mij verder onbekend.
[2] Voor in een kracht van gewijsde gedane beslissing van de civiele rechter (NL: art. 236 lid 1 Rv; BE: art. 28 Ger. W.) kan enkel worden gesproken van een vermeende licentienemer. Vanwege de leesbaarheid is er echter voor gekozen om de term licentienemer aan te houden. Zie ook par. 1.2.
[3] Het watermerk levert in beginsel geen bewijs voor de vraag of de licentienemer ook inbreuk heeft gemaakt op het auteursrecht. Daarvoor is meer bewijs nodig (par. 3.4).

de beveiliging van het watermerk in de gastobjecten moet plaatsvinden is vooral een technische vraag. De juridische vraag is dan of het watermerk onder het bestaande regime voldoende juridische bescherming krijgt tegen het omzeilen en aantasten daarvan (par. 3.5). Het hoofdstuk wordt afgesloten met een samenvatting en conclusie (par. 3.6).

3.2 De rol van het watermerk bij handhaving van auteursrecht

In de afgelopen jaren zijn in Nederland drie grote onderzoeken gepubliceerd waarin verschillende aspecten van up- en downloaden zijn onderzocht.[4] In zowel de nationale als de internationale literatuur is er overeenstemming dat de schaal waarop piraterij plaatsvindt aanzienlijk is.[5] Vanuit het perspectief van de rechthebbende en als grondslag voor de inzet van watermerken is het met name van belang te weten wat de effecten van downloaden op de legale verkoop zijn. Onderzoeken geven echter geen eenduidig antwoord op die vraag. In de meeste onderzoeken komt het beeld naar voren dat downloaden uit illegale bron een negatief effect heeft op de legale verkopen.[6] Ondanks dat de omzet van digitale muziek, film, video en foto's al enige jaren stijgt, kan dit het totale omzetverlies van de fysieke dragers naar verluidt niet compenseren.[7] Onder meer Huygen e.a. 2009 wijzen ook op positieve welvaartseffecten die onder meer ontstaan doordat file sharing burgers toegang geeft tot een breed scala aan cultuurproducten.[8] Piraterij en het downloaden uit illegale bron hebben de politiek ertoe aangezet het handhavingsbeleid te evalueren.[9] Dit heeft echter niet geleid tot een andere visie ten aanzien van de rol die techniek kan spelen bij de handhaving van auteursrecht. Dit onderzoek richt zich verder op een technisch middel in de vorm van het watermerk dat mogelijk zowel kan bijdragen aan het terugdringen van illegaal aanbod als aan de toegang van cultuurproducten door makers het vertrouwen te geven dat hun product beschermd wordt.

---

[4] TNO en IVIR publiceerde in 2009 hun onderzoek Ups-and-downs mede gebaseerd op empirische gegevens uit 2008, naar de economische en culturele gevolgen van filesharing voor muziek, films en games in Nederland (Huygen e.a. 2009). Consideratie publiceerde in 2011 de studie 'Feiten om te delen' dat een kwalitatief onderzoek bevat van de stand van zaken rondom legale en illegale contentdistributie op basis van internationaal literatuuronderzoek (Schermer & Wubben 2011). IViR en CentERdata voerden onder de titel 'Filesharing 2©12' in 2012 een nieuwe meting uit als vervolg op Huygen e.a. 2009 naar het downloaden in Nederland (Poort & Leenheer 2012).

[5] Zie o.m. Frontier Economics, 'Estimating the global economic and social impacts of counterfeiting and piracy', February 2011, dat gebruik maakt van resultaten van het onderzoek van de OECD, 'The Economic Impact of Counterfeiting and Piracy', 2008. Zie voor methodologische problemen bij het OECD echter U.S. Government Accountability Office, 'Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods', April 2010, p. 16 & p. 24.

[6] Zie Schermer & Wubben 2011, p. 109 en de daar aangehaalde onderzoeken (p. 59). Het betreft hier nationale maar ook internationale onderzoeken.

[7] Schermer & Wubben 2011, p. 18. Ook de omzet van fotografen is in 2009 ten opzicht van 2005 gedaald (Legerstee & Verhoog 2010, p. 27). Poort (2014) meldt dat de verkoop van films en series in tegenstelling tot de muziekindustrie in 2013 nog fors af nam. En dat het aantal downloaders van films in 2014 weer hoger lag dan in 2012, en dat dat flink ten koste gaat van de legale consumptie van films op DVD, VoD en TV (Leenheer & Poort 2014, p. 27).

[8] Huygen e.a. 2009, p. 116; Schermer & Wubben 2011, p. 93.

[9] Zie par. 3.3.1.2. Hiermee is niet gezegd dat de overheid zich bij beslissingen altijd zou laten leiden door wetenschappelijk onderzoek (evidence based policy). Zie bijvoorbeeld Hugenholtz (2008b) in zijn open brief aan de Europese Commissie over verlenging van de beschermingsduur van naburige rechten; Van der Leun (2013) die zich de vraag stelt of strafbaarstelling van illegaliteit effectief zal zijn en of iemand dat eigenlijk wil weten?

Het idee achter het centraal gestelde watermerk is dat het watermerk als bewijsmiddel een bijdrage kan leveren aan de handhaving van het auteursrecht door het mogelijk te maken de vermeende licentienemer te traceren.[10] In juridische zin is het dan de vraag of het watermerk als bewijsmiddel kan dienen om een verband te leggen tussen het op internet aangetroffen bestand en de licentienemer.[11]

Watermerken vormt als techniek één van de modaliteiten waarmee regulering van auteursrecht op internet kan worden bewerkstelligd.[12] De inzet van met name de kopieerbeveiliging als een vorm van een Digital Rights Management (DRM) heeft in het maatschappelijk debat over de inzet van techniek veel negatieve associaties opgeroepen over het gebruik van techniek. De kopieerbeveiliging heeft duidelijk gemaakt dat een succesvolle inzet van techniek mede afhankelijk is van de mate waarin consumenten bereid zijn de techniek en de effecten daarvan te accepteren. Hierna wordt om die reden eerst aandacht besteed aan de plaats die het watermerk inneemt in het domein van DRM en de vraag of er aanwijzingen zijn of de consument bereid is het watermerk als techniek te accepteren (par. 3.2.1). Daarna wordt onderzocht of het watermerk aansluiting vindt bij de drijfveren van consumenten om content aan te schaffen en weerstand biedt tegen de drijfveren van uploaders en verspreiders van content om deze te verspreiden. (par. 3.2.2).

3.2.1 Watermerken: DRM met een vriendelijk gezicht

Begin jaren negentig komt de term Digital Rights Management (DRM) op. Hiervan is de kopieerbeveiliging de bekendste en beruchtste vorm.[13] De belangrijkste kritiek op deze vorm van DRM is dat de consument in meer dan enkel zijn illegale handelingen beperkt wordt.[14] Zo kan veel beveiligde content niet overal worden afgespeeld en is het vaak ook niet mogelijk een (auteursrechtelijk toegestane) kopie voor eigen studie of gebruik te maken. Hoewel de kopieerbeveiliging slechts een vorm van DRM is, roept DRM bij het publiek weinig warme gevoelens op. Dit terwijl DRM in essentie niet meer is dan een verzamelbegrip voor het managen van gebruiksrechten van digitale informatiebronnen door een controlesysteem met technologische en organisatorische middelen.[15] DRM heeft in die zin zowel voor- als nadelen,

[10] Voor in een kracht van gewijsde gedane beslissing van de civiele rechter (NL: art. 236 lid 1 Rv; BE: art. 28 Ger. W.) kan enkel worden gesproken van een vermeende licentienemer. Vanwege de leesbaarheid is er echter voor gekozen om de term licentienemer aan te houden. Zie ook par. 1.2.
[11] Het watermerk levert in beginsel geen bewijs voor de vraag of de licentienemer ook inbreuk heeft gemaakt op het auteursrecht. Daarvoor is meer bewijs nodig (par. 3.4).
[12] Zie o.m. Lessig 1999 die bekendheid heeft verworven met vier modaliteiten waarlangs regulering plaatsvindt: markt, recht, sociale normen en architectuur (techniek). Zie ook Prins 2011, p. 1075; Leenes 2010.
[13] Zie voor andere technische voorzieningen uitgebreid de dissertatie van Koelman (2003). Zie voor een overzicht van DRM-systemen die het niet hebben gered o.m. http://opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music. De muziekindustrie heeft de kopieerbeveiliging inmiddels verlaten, maar in filmindustrie en met name in markt voor e-boeken speelt de kopieerbeveiliging nog een rol.
[14] Zie o.m. Guibault & Mom 2007, p. 19.
[15] Zie o.m. Koelman 2003 (diss.); Helberger e.a. 2004.

voor zowel consumenten als producenten.[16] Watermerken maken onderdeel uit van het verzamelbegrip DRM.[17] Vanwege de negatieve reacties die DRM oproept bij het publiek wordt 'watermerken' als technologie ook vaak gepresenteerd als een niet-DRM-oplossing of DRM vrije oplossing. Zo presenteerde Apple al sinds de introductie van iTMS in 2003 haar downloads als DRM-free, terwijl de naam en emailgegevens van de licentienemer aan de aangeboden bestanden werden toegevoegd.[18] Op verschillende websites werd dit aangeduid als het watermerken van bestanden.[19] Ook J.K. Rowling presenteerde haar nieuwe e-boeken van Harry Potter als 'DRM-free' maar kondigde wel aan haar boeken te beveiligen door middel van watermerken die het mogelijk maken de licentienemer te traceren.[20] Deze vorm van DRM heeft in tegenstelling tot de kopieerbeveiliging niet tot grote publieke weerstand geleid. Inmiddels bieden verschillende uitgevers e-boeken aan met watermerken.

Watermerken heeft in die zin inmiddels een eigen plaats gekregen in begrippen als 'social DRM' of 'social watermarking'.[21] Social DRM is gebaseerd op het idee dat de eindgebruiker (en distributeur) niet moet worden belast met gebruiksbeperkingen, zoals bij de kopieerbeveiliging. Piraterij wordt dan als een gegeven beschouwd en de welwillende consument wordt vooropgesteld. Er wordt minder gedacht in termen van bescherming van content door middel van technieken die onrechtmatig gebruik onmogelijk maken, maar in vertrouwen, het opbouwen van banden en daarmee meer in termen van marketing. De band met de klant vormt daarbij de eerste beschermingslaag. De binding bestaat enerzijds uit een goed en klantvriendelijk product en anderzijds in de persoonlijke benadering die tevens de volgende beschermingslaag vormt. De persoonlijke benadering moet dan niet alleen worden gezien in de band met de klant maar ook in het feit dat het product op naam wordt gesteld en de klant dus identificeerbaar is.[22] Het idee daarachter is dat watermerken dan dienen als

[16] Zie o.m. Hugenholtz (2004b) in zijn lezing over 'De toekomst van het auteursrecht: DRM met een vriendelijk gezicht?' Werkers e.a. 2009 (p. 93) laat zien dat ook gebruikers en rechthebbende in België in DRM zowel voor- als nadelen zien.

[17] Zie ook Koelman 2003 (diss.); Helberger 2004; Guibault 2007; Sen Poh & Martin 2009. Ook de termen Electronic Copyright Management Systems (ECMS), Copyright Management Systems (CMS), Automated Rights Management (ARM), Electronic Rights Management Systems (ERMS) of Intellectual Property Rights Management (IPRM) worden gebruikt (Bechtold 2002, p. 2).

[18] Deze werkwijze is nooit bevestigd door Apple. iTMS is het systeem waaruit de i-Tunes worden gedownload. Deze persoonsgegevens waren opgeslagen in de zogenoemde mp4 atom, een ruimte waar in de code ruimte is gereserveerd voor het plaatsen van metadata.

[19] Zie voor de ontdekkingen en kritieken o.m. http://crave.cnet.co.uk/digitalmusic/itunes-plus-everything-you-need-to-know-49300555/ (google: i-tunes, watermarking apple).

[20] Zie o.m. http://www.digitalbookworld.com/2012/why-pottermore-could-change-everything/;
http://www.guardian.co.uk/books/booksblog/2011/jun/23/pottermore-jk-rowling-marketing-genius-harry-potter;
http://www.huffingtonpost.com/2012/03/27/pottermore_n_1383696.html;
http://copyrightandtechnology.com/2012/04/08/the-harry-potter-watermarking-experiment/

[21] Zie o.m. http://www.eburon.nl/dossier_epub;
http://www.eburon.nl/211209_drie_gebruiksvriendelijkere_alternatieven_voor_drm;
http://www.booxtream.com/

[22] Niet iedere ondernemer gebruikt de controlemogelijkheden. Sommigen controleren het internet daadwerkelijk en anderen achten de drempel om gepakt te worden voldoende. Bij Social DRM die nu in e-boeken worden gebruikt wordt bij de aanschaf van het e-boek, de volledige naam van de aankoper in het exemplaar aangebracht. Daarbij accepteert de ene verkoper ook fictieve namen en controleert de ander juist de identificatie van de koper. E.a. mede afhankelijk van de eis van de rechthebbende in de distributie-overeenkomst. Zie voor dergelijk gebruik ook Guibault 2007 en websites als luisterrijk en inmiddels potter.com.

afschrikmiddel waardoor mensen minder geneigd zouden zijn content illegaal te verspreiden.[23]

Bij gebruikers van watermerken leeft doorgaans niet het idee dat watermerken onfeilbaar is. Het adagium dat alles wat digitaal is, te kraken is, geldt ook voor watermerken. Social watermarking richt zich vanuit de handhaving dan ook meer op het eerlijk houden van de betalende en niet uploadende gebruikers dan op de groep die uiteindelijk toch in staat zal zijn de content te kraken en te verspreiden. Watermerken is er in die zin vooral op gericht het verspreidingsproces te vertragen door het lastig(er) te maken de content watermerkvrij te verspreiden. In de markt geeft het de rechthebbende een vorm van bescherming voor zijn werk, terwijl de consument niet beperkt wordt in zijn handelingen.

Het gebruik van watermerken in het verleden alsmede het gebruik van watermerken in de praktijk van e-boeken laat zien dat er weinig reden is om aan te nemen dat watermerken niet door consumenten zullen worden geaccepteerd wanneer deze in andere content zouden worden aangebracht.[24]

In het licht van watermerken en andere technische voorzieningen is het nog interessant om melding te maken van de overwegingen van de voorzieningenrechter en het hof inzake NUV/Tom Kabinet.[25] In de kern gaat het in deze zaak om de vraag of de website Tom Kabinet een onlinemarkt in tweedehands e-boeken mag opzetten en faciliteren. De rechter komt in beide zaken kort gezegd tot de conclusie dat het onduidelijk is of het arrest van het Hof van Justitie EU inzake Usedsoft, waarin besloten ligt dat de verkrijger van een licentie om een computerprogramma voor eigen gebruik te downloaden deze licentie vervolgens ook aan een derde mag overdragen, ook van toepassing is op het in deze zaak voorliggende geval van e-boeken.[26] Dat leidt in beide zaken tot de conclusie dat Tom Kabinet in beginsel niet kan worden belet om een website te exploiteren die de handel in tweedehands e-boeken faciliteert. In beide zaken speelt vervolgens de vraag voor wiens risico het komt dat erop de website ook gehandeld kan worden in illegaal verkregen e-boeken. In beide zaken wordt er dan ook terecht op gewezen dat het Hof in het UsedSoft-arrest heeft opgemerkt dat het moeilijk kan blijken te zijn om na te gaan of een verkochte kopie door de verkoper onbruikbaar is gemaakt, maar dat het aan de distributeur is om voor zoveel mogelijk hiertoe technische beschermings-maatregelen te treffen.[27] De voorzieningenrechter in Amsterdam lijkt dit uit te leggen alsof de

[23] Zo stelt ook Marc Jellema van de website Tom Kabinet in http://www.consumentenbond.nl/test/elektronica-communicatie/overige-elektronica/e-readers/tom-kabinet/.
[24] Zie voor het gebruik van watermerken ook par. 2.2.4.
[25] vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet);
Hof Amsterdam, 20 januari 2015 ECLI:NL:GHAMS:2015:66 (NUV/Tom Kabinet).
[26] vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet), ov. 4.10; Hof Amsterdam, 20 januari 2015 ECLI:NL:GHAMS:2015:66, ov. 3.5.5. Partijen debatteren ter zitting over de vraag of het Usedsoft-arrest (HvJEU 3 juli 2012, zaak C-128/11 van toepassing is waarin het Hof kort gezegd de verkoop van tweedehands software toestaat (digitale uitputting).
[27] HvJEU 3 juli 2012, zaak C-128/11 (UsedSoft), ov. 79: ‘Om dit probleem op te lossen kan de ‘klassieke’ of ‘digitale’ distributeur technische beschermingsmaatregelen, zoals productsleutels, toepassen.’

rechthebbende deze technische beschermingsmaatregelen moet treffen.[28] Het hof stelt dat Tom Kabinet verantwoordelijk is voor het treffen van adequate maatregelen tegen inbreukmakende handelingen omdat zij de verkoop van de boeken faciliteert. In deze procedure heeft het NUV aangegeven dat sommige boeken niet van watermerken zijn voorzien en dat het door de verkoop van deze boeken nagenoeg onmogelijk wordt personen die verantwoordelijk zijn voor handel in illegale e-books te achterhalen.[29] Door erop te wijzen dat het aan de distributeur is om voor zover mogelijk technische beschermingsmaatregelen te treffen lijkt de Nederlandse rechter in navolging van het Europese Hof in UsedSoft te zeggen dat men dan maar moet kiezen voor vormen van beveiliging die het de gebruiker onmogelijk maakt om het boek na een verkoop nog te gebruiken.[30] Dat betekent dat de rechthebbende wordt gedwongen om gesloten systemen aan te bieden. Dat lijkt mij in het licht van de geschiedenis van kopieerbeveiliging niet de gewenste weg.[31] Een samenwerking lijkt mij meer voor de hand liggen. Met het gebruik van watermerken geven de rechthebbenden aan het watermerk een adequaat middel van bescherming te vinden. Een mogelijke oplossing ligt dan in het gebruik van een zogenoemde Trusted Third Party die het mogelijk maakt de naam van de licentienemer te wijzigen door aan de in het watermerk opgenomen code een andere licentienemer te verbinden. Voor een dergelijke oplossing is echter wel samenwerking nodig, zoals Tom Kabinet terecht stelt bij de voorzieningenrechter.[32]

3.2.2 Watermerken in het licht van de drijfveren van up- en downloaders

Watermerken richt zich op het traceren van de identiteit van de licentienemer vanuit de gedachte dat het met die watermerken eenvoudiger is illegaal aanbod met juridische middelen te bestrijden. Onderzoek naar het illegaal aanbod van content op internet wijst uit dat een belangrijk deel afkomstig is van een los verband van goed georganiseerde groepen die worden aangeduid als ‘the scene’.[33] Deze groepen beschikken vaak over muziek en films van goede kwaliteit omdat zij deze veelal verkrijgen bij de bron (productie- en distributieproces).[34] Zij

[28] vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet), ov. 4.10: ‘In dit verband is van belang dat verdergaande beschermingsmaatregelen, die met medewerking van de uitgevers zouden kunnen worden gerealiseerd, niet mogelijk zijn, nu het NUV en GAU ieder overleg hierover weigeren. Overigens heeft het Hof ook in het UsedSoftarrest opgemerkt dat het moeilijk kan blijken te zijn om na te gaan of een verkochte kopie door de verkoper onbruikbaar is gemaakt, maar dat het aan de distributeur is om voor zoveel mogelijk hiertoe technische beschermingsmaatregelen te treffen.’

[29] vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet), ov. 3.2. De kritiek dat er in de praktijk nauwelijks meer verschil valt te maken tussen rechtmatige en onrechtmtige exemplaren is ook al naar voren gekomen in de commentaren op het Usedsoft-arrest..

[30] Zoals de klassieke DRM vormen van Adobe of gesloten systemen zoals die van Amazon.

[31] Overigens kan dit er in de praktijk toe leiden dat uitgevers een model gaan kiezen dat overeenkomsten vertoont met software. De uitputtingsregel gaat immers niet op voor licenties die in duur beperkt zijn (ov . 72 Usedsoft) en geldt ook niet wanneer er sprake is van een dienst in plaats van een product (books as a service).

[32] De voorzieningenrechter rekent het NUV het gebrek aan medewerkering aan. vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet): ‘In dit verband is van belang dat verdergaande beschermingsmaatregelen, die met medewerking van de uitgevers zouden kunnen worden gerealiseerd, niet mogelijk zijn, nu het NUV en GAU ieder overleg hierover weigeren.’

[33] Cuevas e.a. 2011, p. 2; Schermer & Wubben 2011, p. 44.

[34] Zie ook Schermer & Wubben 2011, p. 44.

hebben ook vaak als doel deze werken te verspreiden voor de officiële lanceerdatum.[35] Cuevas e.a. constateren dat 67% van de content op de door hen onderzochte file sharingnetwerken Mininova en Piratebay door slechts 100 bronnen ter beschikking is gesteld en goed is voor 75% van alle downloads.[36]

Naar de drijfveren van uploaders is in tegenstelling tot die van downloaders weinig onderzoek gedaan.[37] Cuevas e.a. maken op basis van hun bevindingen onderscheid tussen drie soorten aanbieders: nep-, altruïstische en op winstgerichte aanbieders. De eerste groep van nep-aanbieders bestaat uit anti-piraterijorganisaties of malafide gebruikers die samen verantwoordelijk zijn voor 30% van de content en 25% van de downloads. Anti-piraterijorganisaties zouden voornamelijk als doel hebben de index te vervuilen, om verspreiding tegen te gaan. Malafide uploaders gebruiken de netwerken voornamelijk om virussen en malware te verspreiden. De tweede groep heeft vooral altruïstische motieven en bestaat uit mensen die geloven in een vrije verspreiding van werken (free culture beweging) dan wel uit gewone gebruikers die (door het protocol) tegelijk uploaden als downloaden.[38] De derde en laatste groep heeft voornamelijk een winstoogmerk. De helft van de top-uploaders heeft als doel om mensen te verleiden om hun website te bezoeken. Deze groep is verantwoordelijk voor 37% van het totale aanbod (van niet-valse torrents) en rond de helft van het totale downloadverkeer van hun dataset.[39] Op basis van het onderzoek van Cuevas e.a. kan geconcludeerd worden dat een kleine groep uploaders verantwoordelijk is voor een groot deel van de beschikbare content. In het algemeen lijkt een deel van de uploaders altruïstische motieven te hebben, maar het belangrijkste deel heeft een winstoogmerk.[40] De drijfveren van uploaders in het algemeen variëren daarmee van altruïsme, competitie en eer tot financiële motieven.[41] Het elimineren van de financiële prikkels door bijvoorbeeld anti-piraterij acties, zou volgens Cuevas e.a. tot een afname van de populariteit van downloadportalen en het BitTorrent ecosysteem kunnen leiden.[42] Vanuit die gedachte opereren veel belangen-organisaties zoals het Nederlandse BREIN en het Belgische BAF wanneer zij pogingen doen om faciliterende websites zoals de The Pirate Bay te sluiten. Het onderzoek van Poort & Leenheer laat echter zien dat het blokkeren van filesharing-site The Pirate Bay in 2012 weinig effect heeft gehad op het gedrag van consumenten.[43]

---

[35] Voor een nadere beschrijving van de wijze waarop de werken verder worden verspreid zie o.m. Schermer & Wubben 2011, p. 44.
[36] Cuevas e.a. 2011, p. 2.
[37] Zie ook Schermer & Wubben 2011, p. 47.
[38] Leiders van de free culture beweging, zoals Lessig streven naar hervorming van het auteursrecht en zijn in beginsel eerder voor wetshervorming of vrijwillige deelname (zie onder meer: Lessig, L. (2004), Free Culture, New York: Penguin Books).
[39] Cuevas e.a. 2011, p. 6.
[40] Zie ook Schermer & Wubben 2011, p. 47.
[41] Zie Torrentfreak (2009), Former movie piracy Scene member speaks out, via: http://torrentfreak.com/former-movie-piracy-scene-member-speaks-out-101029/; Schermer & Wubben 2011, p. 44
[42] Cuevas e.a. 2011, p. 12. Poort (2014) wijst erop dat het illegaal verklaren van downloaden en het tegengaan van illegaal aanbod kan helpen, maar dat goed legaal aanbod de beste remedie is tegen illegaal downloaden.
[43] Poort & Leenheer 2012, p. 5, 37. Zie voor een andere zienswijze en commentaar op Poort & Leenheer 2012, Kuik van Stichting Brein: http://www.anti-piracy.nl/nieuws.php?id=277 .

Onderzoek van Poort & Leenheer (2012) naar het downloaden van muziek, films, series, games en boeken in Nederland wijst uit dat iets meer dan een kwart (27,2%) van de bevolking van 16 jaar en ouder in het afgelopen jaar weleens heeft gedownload uit illegale bron.[44] Muziek blijft daarbij favoriet (21,7%), gevolgd door films en series (18,3%) en op enige afstand games (6,3%) en boeken (6,3). Foto's zijn in dit onderzoek niet meegenomen. Toch komt downloaden uit illegale bron pas op een gedeelde derde plaats als verkrijgingsbron voor content. Op de eerste plaats staat de aankoop van fysieke dragers in een (web)winkel (82,6%), gevolgd door legale alternatieven zoals downloads of streaming (YouTube of Spotify Free). Poort & Leenheer 2012 concluderen dat consumptie van legaal en illegaal aanbod elkaar niet uitsluiten. Zij concluderen dan ook 'wie actief bezig is met muziek, films en series, games of boeken, meer zal downloaden uit illegale bron, maar zal ook meer legaal consumeren en meer afgeleide producten afnemen'.[45] Uit het onderzoek blijkt ook dat er minder muziek uit illegale bron wordt gedownload, maar dat het downloaden van films en series sinds 2008 is toegenomen. De verklaring daarvoor wordt vooral gezocht in het betere legale online muziekaanbod in vergelijking met het aanbod vanuit de filmindustrie.[46] Gezien het aantal alternatieven mag worden verwacht dat nieuwe metingen daar in de toekomst meer duidelijkheid over kunnen geven. Voor het watermerk is vooral van belang dat het onderzoek ook uitwijst dat slechts een kleine minderheid van de bevolking gekocht materiaal uploadt (5%). In het onderzoek is niet onderzocht waarom anderen het materiaal niet uploaden. Het beeld sluit aan bij andere onderzoeken die erop wijzen dat een kleine groep verantwoordelijk is voor het aanbod uit illegale bron.[47] Vanuit het idee dat deze kleine groep lastig is op te sporen en hun activiteiten lastig zijn af te stoppen moet het watermerk vooral dienen om de consument eerlijk te houden en geen content te laten uploaden.

Consumenten hebben in verschillende onderzoeken aangegeven dat de primaire drijfveer voor downloaden uit illegale bron gelegen is in het gratis aanbod.[48] Andere motieven die worden genoemd zijn de mogelijkheid om content eerst uit te proberen, sociale elementen die samenhangen met vinden, ontdekken en delen, het ontbreken van beperkingen (kopieerbeveiliging) en het gebrek aan kwalitatief goed legaal aanbod. De laatste twee argumenten lijken met de tijd te kunnen verdwijnen nu er steeds meer legaal aanbod is met minimale beperkingen.[49] In onderzoek naar de vraag waarom consumenten niet downloaden

[44] Poort & Leenheer 2012, p. 3.
[45] Poort & Leenheer 2012, p. 4, 21.
[46] Poort & Leenheer 2012, p. 5, 35. Deze conclusie sluit aan bij de conclusies uit Noors Onderzoek uit 2013, die de Noorse markt bestudeerde tussen 2008-2012, zo meldt Torrent Freak: http://tweakers.net/nieuws/90284/noors-onderzoek-illegaal-downloaden-keldert-dankzij-legale-alternatieven.html. Ook Poort (2014) komt tot de conclusie dat ontwikkelingen in het legale aanbod op internet de meest aannemelijke verklaring is voor de afname van illegale downloads van muziek en de toename bij films.
[47] Zie Schermer & Wubben 2011, p. 48.
[48] Zie voor een overzicht en bespreking van deze onderzoeken Schermer & Wubben 2011, p. 51. Zie specifiek voor films ook Leenheer & Poort 2014, p. 14, 27. Ondervraagden noemen daar tevens als belangrijkste reden dat de film nog niet in Nederland uit is en op deze manier makkelijk aan hun verzameling kan worden toegevoegd.
[49] Poort (2014) meldt echter dat de verkoop van films en series in tegenstelling tot de muziekindustrie in 2013 nog fors af nam. En dat het aantal downloaders van films in 2014 weer hoger lag dan in 2012, en dat dat flink ten koste gaat van de legale consumptie van films op DVD, VoD en TV (Leenheer & Poort 2014, p. 27).

uit illegale bron worden drijfveren benoemd in termen van kwaliteit van het product, zoekkosten, morele (oneerlijk ten opzichte van makers), juridische (dreiging met sancties) en technische kosten (virussen en malware).[50] Met het watermerk zal de rechthebbende dan vooral een beroep willen doen op de dreiging van juridische kosten.

De gebruiker van watermerken (rechthebbende) zal zich op basis van onder meer eerder genoemd onderzoek moeten realiseren dat hij uiteindelijk een middel inzet voor overtredingen van een kleine groep mensen wiens activiteiten waarschijnlijk nooit helemaal zijn te voorkomen. Het inzetten van watermerken kan afhankelijk van het doel dat men stelt worden vergeleken met de inzet van flitspalen en veiligheidscamera's die ertoe dienen om normconform gedrag te bevorderen voor iedereen. Evenals bij watermerken houdt een deel van de groep zich aan deze regels ook zonder flitspalen, houdt een deel van de groep zich aan de regels vanwege de juridische kosten en houdt een ander deel van de groep zich ongeacht de kosten, niet aan de regels. Deze laatste groep accepteert de daaraan verbonden kosten of probeert via andere middelen aan de sancties te ontsnappen, bij flitspalen bijvoorbeeld door gebruik te maken van een radarverklikker, valse kentekenplaten, of door het ondetecteerbaar maken van de kentekenplaten.[51]

Uploaders zijn er in de regel op uit om de effectiviteit van het watermerk aan te tasten. Dat betekent dat de robuustheid van het watermerk van groot belang is voor het succes ervan. Het watermerk moet meer robuust zijn om aanvallen van deze kleine groep malafide uploaders te weerstaan dan dat nodig zou zijn voor normaal gebruik door de gemiddelde consument. Evenals bij veel beveiligingsmaatregelen, zoals tegen woninginbraak of cybercriminaliteit geldt dat deze gericht zijn op een kleine groep 'professionele' overtreders. Gezien de ervaringen bij andere technieken, is er weinig reden om aan te nemen dat watermerken wel een waterdichte oplossing zou bieden. De winst is voor de rechthebbende dan vooral gelegen in de tijd tussen het op de markt brengen en de kraak. Dit is met name van belang voor producten waarbij de waarde groot is in het begin van hun levenscyclus, zoals bij een nieuwe film die in de (thuis)bioscoop wordt vertoond.

Het watermerk sluit in beginsel goed aan bij de eerder genoemde drijfveren van consumenten. Het beperkt hen niet in hun handelen en zij kunnen daardoor ook het sociale element van content volledig benutten. Aan de preventieve zijde doet het watermerk nog het meest een appèl op de morele en juridische kosten. Daarvoor is wel een goede voorlichting noodzakelijk omdat het watermerk onwaarneembaar is en in tegenstelling tot waarneembare watermerken de consument niet voortdurend wijst op het risico van deze kosten.[52] Ook hier is een

[50] Zie voor een overzicht en bespreking van deze onderzoeken Schermer & Wubben 2011, p. 53. Het is overigens maar de vraag welke sancties direct een grote invloed zouden hebben op het download gedrag van consumenten. Arnold e.a. 2014 tonen aan dat de Franse Hadopi-wetgeving, die mogelijkheden bood om herhaaldelijke downloaders van het internet af te sluiten, nauwelijks effect heeft gehad.
[51] Zie ten aanzien van de voorlichting ook par. 5.3.2.1 over informatieplichten inzake privacy .
[52] Zie ook Bill Rosenblatt in zijn blogpost over Harry Potter: http://copyrightandtechnology.com/2012/04/08/the-harry-potter-watermarking-experiment/

vergelijking te maken met de eerder genoemde flitspalen en cameratoezicht die zowel duidelijk zichtbaar als onzichtbaar normconformgedrag willen bevorderen. Bij onzichtbare flitspalen en camera's geldt evenals voor het watermerk dat de preventieve werking weleens de sterkste vorm van regulering van gedrag zou kunnen opleveren. Daartegenover staat dat groepen die worden aangeduid als de 'scene' erop uit zijn om DRM-beveiligingen buiten werking te stellen en zich niet laten afschrikken door (juridische) sancties. Dit laatste brengt met zich mee dat watermerken ook niet langer preventief werken. Watermerken met een traceerdoel verhinderen immers geen enkele gebruiker om het werk op internet te plaatsen, maar bieden slechts de mogelijkheid een verband te leggen met de licentienemer en het op internet geplaatste werk. Het watermerk dient dan ook voornamelijk het doel om de groep 'eerlijk' betalende gebruikers ook 'eerlijk' te houden en inspelend op de angst voor sancties met het watermerk om te voorkomen dat ook deze groep werken gaat verspreiden.

3.3 De plaats van watermerken in het handhavingsbeleid

Vanwege de vergaande mate waarin het auteursrecht gebaseerd is op internationale verdragen en geharmoniseerd is door verschillende Europese richtlijnen en uitspraken van het HvJ EU daarover hebben de nationale wetgevers een beperkte beleidsruimte voor het vinden van oplossingen voor de problemen waarvoor het internet het auteursrecht heeft geplaatst.[53] De Nederlandse overheid ziet in de Europese regelgeving en internationale verdragen eveneens een brede consensus over de meerwaarde van exclusieve rechten en vergoedingsrechten van makers waarin de grondslag voor handhaving van het auteursrecht moet worden gevonden.[54] Het Europese en nationale (handhavings)beleid vertaalt zich veelal in de vorm van wetgeving en de mate waarin nationale overheden bereid zijn het strafrecht en de bijbehorende opsporingsinstanties in te zetten voor de handhaving van het auteursrecht. Naast het gedrag van de consument en uploader is dit een andere factor die van invloed is op de wijze waarop het watermerk kan bijdragen aan de handhaving van het auteursrecht. Vanwege de Europese invloed op het nationale beleid wordt eerst de regelgeving vanuit de Europese Unie op hoofdlijnen besproken en worden daarna vergelijkenderwijs de uitgangspunten van het beleid in Nederland en België besproken (par. 3.3.2).[55] Daaruit zal blijken dat in beide landen voornamelijk de civielrechtelijke handhaving een belangrijke rol speelt en dat het watermerk

[53] Zie internationaal o.m. Berner Conventie (BC), TRIPs-Verdrag (TRIPs) en in Europa o.m. de Softwarerichtlijn (2009/24/EG); Beschermingstermijn (2006/116/EG); Verhuurrichtlijn, (2006/115/EG); Handhavingsrichtlijn (2004/48/EG); Volgrechtrichtlijn (2001/84/EG); Auteursrechtrichtlijn (2001/29/EG); Databankrichtlijn (96/9/EG); Satelliet- en kabelrichtlijn (93/83/EEG). Zie de beleidsbrief over het auteursrecht aan de TweedeKamer van de ministers van Justitie, Economische Zaken en OCW d.d. 20 december 2007 (Auteursrechtbeleidsbrief), p. 2. Zie ook Hugenholtz 2008 AA, p. 581.

[54] Beleidsbrief 20 december 2007, p.2.

[55] De vraag of vanuit een intrinsiek juridisch perspectief gezien de (klassieke) intellectuele eigendom door zijn inrichting en systematiek blijk geeft van een impliciete voorkeur voor handhaving op het niveau van het handelsverkeer is buiten beschouwing gelaten. Het zijn echter de nationale overheden die in de context van het Europese recht zelf expliciet bepalen op welke wijze zij het auteursrecht willen handhaven. Dat maakt in het licht van dit onderzoek de vraag naar de impliciete voorkeur of onderliggende rationales minder interessant. In Nederland heeft vooral Grosheide aandacht gevraagd voor de verschuiving van een individu-auteursrecht naar een entrepreneurial copyright.

door de rechthebbende zelf wordt ingezet. Vervolgens zal dan ook worden ingegaan op de wijze waarop particulieren in Nederland en België omgaan met de handhaving van het auteursrecht en de rol die het watermerk daarin kan spelen (par. 3.3.3).

3.3.1 Handhavingsbeleid van overheidswege

3.3.1.1 Europese Unie

De handhaving van intellectueel eigendomsrecht staat duidelijk op de agenda van de Europese Commissie. Intellectuele rechten worden als een belangrijke stimulans gezien voor de creativiteit en innovatie van de interne markt en economie.[56] Zowel de Europese Commissie als het Europees Parlement delen de zorg dat online auteursrechtinbreuken een probleem vormen en dat het illegale aanbod van content nieuwe legale diensten in de weg staat.[57]

In 2004 werd een aparte Handhavingsrichtlijn ingevoerd voor intellectuele rechten.[58] Verderop wordt daarop nader ingegaan. Daarnaast wordt er al jaren gezocht naar een juridisch kader dat binnen de grenzen van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest) en met inachtneming van de belangen van de eindgebruikers het mogelijk maakt om een effectief raamwerk te creëren om auteursrechtinbreuk op het internet effectief te bestrijden. Uit de eerste evaluatie van de Handhavingsrichtlijn concludeert de Commissie dat de richtlijn in het algemeen een significant positief effect heeft op de civielrechtelijke bescherming van intellectuele-eigendomsrechten in Europa, maar niet is ontworpen vanuit de zorg over de internet gerelateerde problemen met de handhaving van intellectuele eigendomsrechten.[59] In 2007 werd door Japan en de Verenigde Staten het initiatief genomen om buiten de bestaande internationale organisaties om tot een multilateraal verdrag te komen met als doel tot samenwerking en een effectiever juridisch raamwerk voor de bestrijding van namaak en (internet)piraterij te komen. Dit zogeheten Anti-Counterfeiting Trade Agreement (hierna: ACTA) werd op 4 juli 2012 door het Europees Parlement verworpen.[60] In deze

[56] Zie o.m. 'A Single Market for Intellectual Property Rights Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe'. Brussels, 24.5.2011. COM(2011) 287 (http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_en.pdf). Accent op digitale omgeving. http://ec.europa.eu/internal_market/iprenforcement/directives_en.htm

[57] Zie o.m. de aangenomen resolutie door het Europees Parlement van 22 September 2010 on enforcement of intellectual property rights in the internal market, 2009/2178/INI, waarin zelfs gesteld wordt dat online auteursrechtbreuken verontrustende vormen hebben aangenomen (onder J).

[58] Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (Pb.EU L 157 van 30 april 2004). Gerectificeerd op 2 juni 2004 (Pb. EU L195/16); COM (2011) 287, p. 19 – A Single Market for Intellectual Property Rights. Zie voor een evaluatie van de handhavingsrichtlijn (Brussel, 10 januari 2011, kenmerk 5140/11) en de Nederlandse reactie daarop Bijlage bij Kamerstuk 29838 nr. 30.

[59] Zie voor een evaluatie van de Handhavingsrichtlijn (Brussel, 10 januari 2011, kenmerk 5140/11) en de Nederlandse reactie daarop Bijlage bij Kst II 29838 nr. 30.

[60] De grote vrees voor het opnemen van een zogenoemde 'three strikes you're out' en controle bij de douane van notebooks waren in het voorgelegde verdrag niet langer opgenomen. Eerder verwierp het Nederlandse Kabinet ACTA al (brief van Verhagen en Teeven van 25 juni 2012 aan TK). België wilde tijdens het vragenuurtje op 16 februari 2012 bij monde van minister Vande Lanotte eerst een studie verrichten naar de impact van ACTA op de

ACTA-discussie speelde met name het gebrek aan transparantie rondom de onderhandelingen en zorgen over de privacy van burgers een belangrijke rol. De Commissie had eerder al aan het Hof van Justitie EU (hierna: HvJ EU) advies gevraagd over de verenigbaarheid van ACTA met de Verdragen en in het bijzonder met het Handvest.[61] Het Parlement verwierp ACTA al voordat het HvJ EU hierover een uitspraak heeft gedaan. Ondanks het verwerpen van dit multilaterale verdrag blijft de Commissie zoeken naar een wijze waarop internet gerelateerde problemen met de handhaving van intellectuele eigendomsrechten kunnen worden aangepakt.

Duidelijk is dat er de afgelopen jaren in de verschillende discussies minder aandacht is voor de inzet van techniek als bijdrage aan de handhaving van het auteursrecht dan aan het begin van deze eeuw.[62] De gedachte is niet langer dat techniek een vooraanstaande rol zal spelen bij het reguleren van de handhaving van het auteursrecht. Die gedachte heeft plaatsgemaakt voor een meer bescheiden rol voor techniek, mede vanuit het idee dat elke techniek te kraken is. Hiermee is de aandacht voor techniek niet verdwenen, maar is de betekenis van techniek in het handhavingsdebat veranderd. Dit laat onverlet dat juridische beschermingsmaatregelen tegen het omzeilen en verwijderen van technische middelen nog steeds van kracht zijn (par. 3.5). De huidige discussie spits zich mede in het licht van het Handvest toe op de vraag in hoeverre de inzet van techniek inbreuk maakt op Europese grondrechten.[63]

Een belangrijk instrument in het kader van de handhaving van intellectuele eigendomsrechten is de Handhavingsrichtlijn.[64] In deze richtlijn zijn in navolging van met name het TRIPs-Verdrag van 1994 minimumbepalingen opgenomen voor de handhaving van intellectuele eigendomsrechten.[65] De Handhavingsrichtlijn is van toepassing op maatregelen, procedures en rechtsmiddelen die nodig zijn om de handhaving van de in deze richtlijn bedoelde intellectuele eigendomsrechten te waarborgen, waaronder het auteursrecht (art. 1 Rl.). Deze richtlijn harmoniseerde de handhavingsmiddelen die een rechthebbende kan inzetten in IE-geschillen in de lidstaten van de EU en omvatten onder meer bewijsbeschermings-maatregelen, een ex-parte verbod en een 'volledige' proceskostenveroordeling.[66] Met name

nationale wetgeving. Voor meer achtergronden rondom de totstandkoming van ACTA verwijs ik o.m. naar Hagemans 2011.

[61] Zie adviesverzoek van 10 mei 2012, EC A-001/12 uit hoofde van art. 218, lid 11 VWEU.

[62] Zie ook het onderzoek van Werkers e.a. 2009, p. 102 waarin Belgische rechthebbenden een meer bescheiden rol zien voor DRM-toepassingen.

[63] Zie par. 5.3.1.

[64] Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (Pb.EU L 157 van 30 april 2004). Gerectificeerd op 2 juni 2004 (Pb. EU L195/16). Zie voor een rechtsvergelijkende analyse van deze regeling o.m. SEC (2010) 1589, 22 December 2010.

[65] Agreement on Trade Related Aspects of Intellectual Property Rights oftewel de Overeenkomst inzake de handelsaspecten van de intellectuele eigendom (TRIPs), Pb.L. 336, 23 december 1994. De goedkeurig van dit verdrag vond in Nederland plaats Trb. 1995, 130 en in België bij wet van 23 december 1994 (BS 23 januari 1997).

[66] Zie voor kritische beschouwingen o.m. de door 36 IE-hoogleraren ondertekende " de 'Professor's Letter' van 36 hoogleraren IE: W.R. Cornish e.a. 2003; Huydecoper 2004; Hugenholtz 2004a. De kritiek ziet op de richtlijn voorziet met name op de reikwijdte, subsidiariteit en de proportionaliteit. Waarbij Hugenholtz zich afvroeg

deze laatste maatregel was voor zowel Nederland als België nieuw en heeft directe consequenties voor procederende partijen en met name voor de verliezende partij. Op grond van artikel 14 Rl. geldt inmiddels in beide landen dat redelijke en evenredige gerechtskosten en andere kosten die de in het gelijkgestelde partij heeft gemaakt, door de verliezende partij zullen worden gedragen, tenzij de billijkheid zich daartegen verzet.

In Nederland is de richtlijn geïmplementeerd in een nieuwe Titel 15 van het Wetboek van Burgerlijke Rechtsvordering: Van rechtspleging in zaken betreffende rechten van intellectuele eigendom (art. 1019 e.v. Rv). Artikel 14 van de richtlijn is geïmplementeerd in art. 1019h Rv dat het mogelijk maakt dat de in het ongelijkgestelde partij desgevorderd wordt veroordeeld in redelijke en evenredige gerechtskosten en andere kosten die de in het gelijkgestelde partij heeft gemaakt, tenzij de billijkheid zich daartegen verzet.[67] Inmiddels zijn er in Nederland door de Rechtspraak in overleg met de Nederlandse Orde van Advocaten indicatietarieven vastgesteld zodat partijen een handvat hebben om de redelijkheid van de gemaakte proceskosten te kunnen beoordelen en om het mogelijke kostenrisico beter in te kunnen schatten in een vroeg stadium van een procedure.[68] Ook maken partijen in toenemende mate afspraken over de hoogte van de te vergoeden proceskosten.[69]

De implementatie van de Handhavingsrichtlijn in België is geregeld in drie wetten.[70] Artikel 14 van de richtlijn is niet omgezet in wetgeving. De wetgever is van mening dat de hier bedoelde kosten deels zijn opgenomen in art. 1017 Gerechtelijk Wetboek (Ger. W.).[71] Voor de kosten van advocaten en experts wordt verwezen naar jurisprudentie en het gewijzigde artikel 1022 Ger.W., waarin een forfaitaire tegemoetkoming in de kosten en erelonen van de advocaat van de in het gelijkgestelde partij wordt toegekend (rechtsplegingsvergoeding).[72] In

waarom inbreuk op IE-rechten ernstiger zouden dan zijn dan schending van 'normale' vermogensrechten. En waarom Microsoft en Louis Vuitton over meer procesrechtelijke bevoegdheden moeten beschikken dan de slachtoffers van een milieudelict of een verkeersongeval?

[67] Zie voor een kritische bespreking van de implementatie en interpretatie van artikel 14 Handhavingsrichtlijn in Nederland o.m. Vrendenbarg 2013.

[68] Indicatietarieven in IE-zaken (11 oktober 2010). Nodeloos gemaakte kosten worden niet vergoed, bijvoorbeeld omdat gedaagde bereid is een onthoudingsverklaring te tekenen voor de zitting (Rb. 's-Gravenhage 8 april 2009, IEF 8759 (Present Sieraden/X). Voor een beroep op de volledige onkostenvergoeding zijn meer omstandigheden van belang. Zie o.m. Hof Amsterdam 16 maart 2010, ECLI:NL:GHAMS:2010:BL7920, IER 2010, 78 m.nt. MdCB (e-Donkey), ov. 3.13: '(…) waarbij een professionele belangenorganisatie staat tegenover een (…) thuiswonende student die zich als hobby met het ontwikkelen van de in geding zijnde site heeft beziggehouden.. Zie voor een korte bespreking van (alle relevante) arresten van de Hoge Raad en het Europese Hof van Justitie over artikel 1019h Rv / 14 Handhavingsrichtlijn', o.m. Vrendenbarg 2013 en over het vaststellen van de schade Sandvliet & Engelfriet 2012. Zie voor een toepassing van de indicatietarieven o.m. Olieslagers & Van Gompel 2014.

[69] Vrendenbarg 2013, p. 160.

[70] Wet van 9 mei 2007 betreffende de burgerrechtelijke aspecten van de bescherming van intellectuele eigendomsrechten BS 10 mei 2007 (err. BS 15 mei 2007), in werking getreden op 10 mei 2007; de wet van 10 mei 2007 betreffende de aspecten van gerechtelijk recht van de bescherming van intellectuele eigendomsrechten BS 10 mei 2007 (err. BS 14 mei 2007), in werking getreden op 1 november 2007; Wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten (BS. 18 juli 2007) in werking getreden op 1 oktober 2007.

[71] Parl.St. Kamer 2006-2007, nr. 2943/001, p. 18.

[72] Cass. 2 september 2004, RW 2004, 5, m.nt. C. Clijmans; Wet van 21 april 2007 betreffende verhaalbaarheid van de erelonen en kosten verbonden aan de bijstand van een advocaat (welke art. 1022 Ger. W. wijzigde). Zie

tegenstelling tot de Nederlandse situatie worden de forfaitaire basisbedragen bij KB vastgesteld. Het is partijen verder bij wet verboden om de proceskostenvergoeding contractueel uit te sluiten. De rechter kan op grond van een appreciatiebevoegdheid het basisbedrag aanpassen op grond van vier door partijen aan te voeren gronden: de financiële draagkracht van de verliezende partij, de complexiteit van de zaak, de contractueel bepaalde vergoedingen en het kennelijk onredelijke karakter van de situatie. De rechtsplegings-vergoeding sluit uit dat de kosten en het honorarium van een advocaat nog op een andere, aanvullende wijze worden verhaald. De kosten van een deskundige en de kosten die gepaard gaan met het opsporen van een inbreukmaker vallen niet onder deze wettelijke beperking en zijn in beginsel dus volledig verhaalbaar.[73] Deene komt tot de conclusie dat hoven en rechtbanken in België moeite hebben om hoge rechtsplegingsvergoedingen toe te wijzen en hier in de praktijk op een onjuiste en tegenstrijdige wijze mee omgaan.[74]

In zowel de Nederlandse als Belgische literatuur is op verschillende gronden kritiek geweest op de implementatie van handhavingsrichtlijn in de nationale wetgeving.[75] In de praktijk lijkt de rechter op basis van de indicatie tarieven (NL) of forfaitaire basisbedragen (BE) per geval te beoordelen wat in het voorliggende geval moet worden verstaan onder redelijke en evenredige gerechtskosten.[76] Dat kan er in de praktijk toe leiden dat er mogelijk sprake is van rechterlijke willekeur bij de toepassing van de proceskostenregel die rechtsonzekerheid tot gevolg heeft. Of hiervan in de praktijk ook sprake is, is bij gebrek aan specifiek onderzoek nog onduidelijk.[77] Voor dit onderzoek is het nu slechts van belang aan te tonen dat er in ieder geval in Nederland in beginsel in IE-zaken door de rechter een hogere proceskosten-vergoeding kan worden uitgesproken dan gemiddeld in andere civiele zaken het geval is. Dat gegeven maakt de gevolgen van het verliezen van een procedure groter.[78] Het maakt tevens het belang van het hebben van betrouwbaar bewijs groter. Niet alleen voor het winnen van een zaak in een procedure maar ook wanneer men de wederpartij wil bewegen tot een schikking. Het verliezen van de procedure is immers veel duurder.

In de navolgende paragrafen zal nader worden ingegaan op de vraag hoe nationale wetgevers de Europese richtlijnen uiteindelijk hebben vertaald naar nationaal beleid inzake de

KB van 26 oktober 2007 tot vaststelling van het tarief van de rechtsplegingsvergoeding bedoeld in artikel 1022 van het Gerechtelijk Wetboek en tot vaststelling van de datum van inwerkingtreding van de artikelen 1 tot 13 van de wet van 21 april 2007 betreffende de verhaalbaarheid van de erelonen en de kosten verbonden aan de bijstand van de advocaat. Gepubliceerd in BS 9 november 2007.

[73] Zie uitgebreid Deene 2011, pp. 946-953.

[74] Deene 2011, p. 953. Zie voor een rechtsvergelijking met o.m. België ook Van Vlooten 2011; SEC (2010) 1589, 22 December 2010.

[75] Zie voor Nederland o.m. Vrendenbarg 2013 en voor België Deene 2011 en de daar aangehaalde literatuur.

[76] Zie naar Nederlands recht o.m. Sandvliet & Engelfriet 2012, p. 208.

[77] Ook Vrendenbag (2013) verwijst nergens naar onderzoek waaruit blijkt dat er sprake is van rechterlijke willekeur. Zij lijkt die stelling te baseren op op uitspraken die zijn gedaan tijdens de PAO cursus 'Praktisch Procederen in IE-zaken' op 23 en 30 mei te Leiden (p. 161).

[78] Zo geeft Vrendenbag (2013, p. 161) aan dat sommige advocaten stellen dat de proceskostenregeling ertoe leidt dat met name minder vermogende cliënten eerder afzien van een procedure.

handhaving van auteursrecht en naburige rechten om uiteindelijk de plaats van het watermerk in het handhavingsbeleid van zowel de overheid als particulieren te kunnen bepalen.

3.3.1.2 Nederland

De Nederlandse overheid heeft in haar beleid inzake de handhaving van auteursrecht en naburige rechten traditioneel een voorkeur voor zelfregulering en private rechtenuitoefening, waarbij civielrechtelijke handhaving als vertrekpunt dient en de strafrechtelijke handhaving als sluitstuk.[79]

In 2011 formuleerde het kabinet haar nieuwe auteursrechtbeleid in de zogenoemde Speerpuntenbrief. Het kabinet neemt hierbij als uitgangspunt dat het auteursrecht een stimulans moet zijn voor creativiteit en innovatie, en geen obstakel.[80] Het auteursrecht moet bijdragen om de economische waarde van dat recht, ook in de digitale wereld te vergroten, waarbij rechthebbenden in staat moeten zijn geld te verdienen en consumenten toegang moeten hebben tot een breed en gevarieerd legaal aanbod van kunst en cultuur.[81] Het kabinet wil daartoe nieuwe bedrijfsmodellen op internet bevorderen, en beschermen door een nieuw wetsvoorstel op basis waarvan opgetreden kan worden tegen inbreukfaciliterende websites. Zij wil zich tevens herbezinnen op de thuiskopie-exceptie.[82] De gedachte hierachter is dat de legale markt volgens het kabinet sterk gehinderd wordt door grootschalige en kosteloze uitwisseling van bestanden. Het beleid moet zich niet richten op consumenten die op beperkte schaal up- en downloaden, omdat het niet effectief is en rechtsongelijkheid creëert nu niet iedereen kan worden aangesproken.[83] De discussie heeft zich thans toegespitst op twee mogelijkheden: handhaven of heffen. In de huidige situatie is het in beginsel toegestaan om kopieën te maken van een werk voor eigen oefening, studie of gebruik.[84] Dit wordt ook wel aangeduid als privé-kopiëren of de thuiskopie-exceptie. Het was vóór de uitspraak van het HvJ EU inzake ACI Adam/Stichting De Thuiskopie in Nederland niet relevant of het auteursrechtelijke beschermde werk uit legale of (evident) illegale bron werd verkregen.[85] Het Hof van Justitie EU kwam echter tot het oordeel dat met name artikel 5, lid 2, sub b juncto

[79] Dit zoals toegelicht in de auteursrechtbeleidsbrief van 2007 en brief over rechtshandhaving op internet uit 2008; Brief van de Ministers van Justitie, Economische Zaken en Onderwijs, Cultuur en Wetenschap van 20 december 2007 inzake auteursrechtbeleid, TK 2007-2008, 29 838, nr. 6 herdruk, p. 3; Brief van de Minister van Justitie van 14 april 2008, Naar een veiliger samenleving, TK 2007-2008, 28 684, nr. 133.
[80] Speerpuntenbrief auteursrecht 20©20, p. 2. Herhaald in het Verslag van een schriftelijk overleg. Vastgesteld 14 november 2013, nr, 29 838 Auteursrechtbeleid.
[81] Speerpuntenbrief auteursrecht 20©20, p. 3. Zie voor de economische waarde van het auteursrecht o.m. SEO en onderzoek wisselwerking auteursrecht en mededinginsgrecht.
[82] Speerpuntenbrief auteursrecht 20©20, p. 8. Voor het watermerk is de discussie over de thuiskopieheffing in zoverre nog van belang dat wanneer de thuiskopievergoeding als een compensatie mag worden gezien en er sprake is van een legalisering en is er minder ruimte voor handhaving bij consumenten.
[83] Speerpuntenbrief auteursrecht 20©20, p. 9.
[84] Zie art. 16b en 16c Aw.
[85] HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie). Zie voor gerechtelijke uitspraken daarvoor: o.m. Hof 's Gravenhage, 15 november 2010, FTD/Eyeworks, ECLI:NL:GHSGR:2010: BO3980, IER 2011, 28 m. nt. K.J. Koelman, ov. 5.16.; Rb. Haarlem, 9 februari 2011 ECLI:NL:RBHAA: 2011:BP3757 (FTD/Brein). Zie ook de Minister in Nota n.a.v. het Verslag, TK 2002-2003, 28482, nr. 5, p.32/33.

lid 5 van richtlijn 2001/29/EG in de weg staat aan een nationale wettelijke regeling, die geen onderscheid maakt tussen de situatie waarin de bron van een voor privégebruik vervaardigde reproductie geoorloofd is, en de situatie waarin deze bron ongeoorloofd is. Het kabinet heeft na deze uitspraak van het HvJ EU de Tweede Kamer en door het openbaar maken van deze brief ook een breder publiek over deze uitspraak geïnformeerd.[86] Het kabinet herhaalt in haar brief dat handhaving van het auteursrecht eerst en vooral een privaatrechtelijke aangelegenheid is.[87] Tegelijk constateert het kabinet dat privaatrechtelijke handhaving in de privésfeer van gebruikers technisch gezien niet goed mogelijk is, mede in het licht van het recht op privacy. Doordat het HvJ EU in deze uitspraak een reproductie uit een ongeoorloofde bron niet als een uitzondering voor privé-kopiëren kwalificeert, hebben gebruikers op grond van de auteurswet vooraf toestemming van de rechthebbende nodig om het werk openbaar te maken. Volgens het kabinet kan op grond van dit arrest het aanbieden van diensten die het reproduceren van werken uit ongeoorloofde bron faciliteren een onrechtmatige daad opleveren, waardoor internetsites eenvoudiger kunnen worden aangepakt. Als gevolg daarvan verwacht het kabinet dat het groeiende legale aanbod op internet minder oneerlijke concurrentie zal ondervinden en het legale aanbod voor consumenten daardoor verder zal verbeteren. Het eerder door het kabinet voorgestelde download verbod waarin het kopiëren voor privédoeleinden uit evident illegale bron werd verboden (2010), en dat eerder door een motie van D66 en de PvdA werd verworpen (2012), is hiermee een juridisch feit geworden.[88] Aangenomen mag worden dat het handhavingsbeleid hierdoor niet veranderd is en het kabinet nog steeds van mening is dat de overheid niet zelf achter de individuele downloaders aangaat.[89] De uitspraak heeft in zoverre gevolgen voor de handhavingspraktijk, dat het nu geheel aan de rechthebbende is overgelaten of zij individuele downloaders juridisch willen aanspreken op hun gedrag of niet (zie par. 3.3.2).

Het niet strafrechtelijke vervolgen van individuele downloaders is een beleidskeuze die mede samenhangt met het maken van keuzes (prioritering) die nodig zijn bij het inzetten van het strafrechtelijk opsporings- en vervolgingsapparaat. De wettelijke mogelijkheid om het auteursrecht strafrechtelijk te handhaven bestaat reeds. Sinds 1973 kan het Openbaar Ministerie (hierna: OM) ambsthalve opsporings- en vervolgingsactiviteiten instellen.[90]

[86] Brief van 17 april 2014 inzake Arrest ACI Adam B.V. e.a. tegen Stichting de Thuiskopie en Stiching Onderhandelingen Thuiskopie vergoeding.
[87] Brief van 17 april 2014 inzake Arrest ACI Adam B.V. e.a. tegen Stichting de Thuiskopie en Stiching Onderhandelingen Thuiskopie vergoeding, p. 4.
[88] Kamerstukken II 2010/11, 29838, nr. 29, p 7. Onderzoek in Zweden waar een vergelijkbaar verbod is ingevoerd, namelijk zonder handhaving bij consumenten laat zien dat ervoor de verschillende soorten content verschillen bestaan in effecten en dat het dalend gebruik van filesharing slechts tijdelijk was (Consideratie 2011, p. 127 onder verwijzing naar Adermon & Liang 2010, p. 18. A. Adermon & C.Y. Liang, Piracy, Music and Movies: A Natural Experiment. IFN Working Paper No. 854, 2010).
[89] Speerpuntenbrief auteursrecht 20©20 van 11 april 2011, p. 9; TK, 38e vergadering, 20 december 2011.
[90] Richtlijn voor Strafvordering Intellectuele-Eigendomsfraude (2010R020), Stc. 16 december 2010, nr. 20092, nr. 3.3 (geldigheidsduur: 31-12-2014). Voor 1973 was er sprake van een klachtdelict. Zie voor de totstandkomingsgeschiedenis o.m. het rapport van de Interdepartementale Werkgroep Piraterij (1984), Piraterij van Auteursrechtelijk beschermde werken, Staatsuitgeverij 1984, en verder zie o.m. Spoor, Verkade & Visser 2005, p. 533. en de daar aangehaalde literatuur.

Overigens wordt dit door de politie en het OM nauwelijks gedaan.[91] Ook het OM neemt als uitgangspunt dat in beginsel civielrechtelijke handhaving door de rechthebbende zelf voorop dient te staan. De privaatrechtelijke (IE-) regelingen bieden daar volgens het College van procureurs-generaal genoeg aanknopingspunten voor.[92] De inzet van het strafrecht dient in Nederland ten aanzien van het auteursrecht duidelijk als ultimum remedium. Bij de vraag in welke gevallen het strafrecht wel in aanmerking komt, kan worden aangesloten bij die gevallen waar het algemeen belang in het geding komt. Daarbij kan worden gedacht aan bedreiging van de volksgezondheid of de veiligheid van de samenleving, grootschalige namaak en piraterij (gepleegd in beroep of bedrijf) die de markt verstoren, het bestaan van aanwijzingen van betrokkenheid van criminele organisaties of georganiseerde criminaliteit of bij recidive.[93] De strafrechtelijke opsporingsactiviteiten van zogenoemde 'Intellectuele Eigendomsfraude' is geconcentreerd bij een team van de Fiscale Inlichtingen- en Opsporingsdienst/Economische Controledienst (hierna: FIOD), die worden aangestuurd door het functioneel parket van het OM. Hiervoor is ook een speciale Officier van Justitie aangesteld.

De opsporing en handhaving van auteursrechtinbreuk ligt daarmee in Nederland voornamelijk in handen van private partijen, zoals de individuele rechthebbende of organisaties zoals Stichting Brein (hierna: Brein) of Buma/Stemra. Rechthebbenden of organisaties die optreden namens deze rechthebbende kunnen, nadat zij vermeende inbreukmakers hebben opgespoord, of een civiele procedure beginnen of wanneer zij voor een strafrechtelijke traject kiezen het bewijs overdragen, eventueel met tussenkomst van de FIOD, aan het OM. Het is uiteindelijk ook het OM dat zelfstandig over de vervolging moet beslissen.[94]

Een aan privacy gerelateerd punt betreft het handhavingsmodel dat het kabinet in het kader van het handhaven van auteursrecht voor ogen staat.[95] In dit model wordt als uitgangspunt gehanteerd dat de overheid niet wil handhaven bij consumenten die op beperkte schaal bestanden up- en downloaden. Aangezien het kabinet de civiele handhaving van auteurs-rechten als uitgangspunt neemt kan de rechthebbende deze consument zelf wel aanpakken en ontloopt de burger evenals nu het geval is strafrechtelijke vervolging.[96] Het kabinet vervolgt haar zienswijze door te stellen: 'Als rechthebbenden hun rechten willen beschermen, dan kan dat door gebruik te maken van technische voorzieningen die werken beschermen of waarborgen dat deze alleen tegen betaling beschikbaar zijn (legaal aanbod). Er komen

[91] Zie ook Spoor, Verkade & Visser 2005, p. 533. Ook de Minister was bij MvA (bij het wetswijzigingen i.v.m. de piraterijrichtlijn 3295/94 EK 1998–1999, 25 474, nr. 6b, p. 2) ten aanzien van het invoeren of wijzigen van strafrechtelijke bepalingen al beleidsmatig van oordeel dat er onvoldoende reden is om de verwachting te scheppen dat politie en justitie aan dergelijk optreden prioritaire aandacht gaan besteden.
[92] Aanwijzing intellectuele-eigendomsfraude (2005A022) van het College van procureurs-generaal, Stc. 9 januari 2006, nr. 6, pag. 10 (laatstelijk verlengd tot 31-01-2016; Stc 2010, nr. 1021), nr. 1.
[93] Aanwijzing intellectuele-eigendomsfraude (2005A022) van het College van procureurs-generaal, Stc. 9 januari 2006, nr. 6, pag. 10 (laatstelijk verlengd tot 31-01-2016; Stc 2010, nr. 1021), nr. 2. (vgl. ook art. 140 WvSr).
[94] Hof 's-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010:BO8239 m.nt. Duker, AMI 2011/5, nr. 9, (e-donkey).
[95] Speerpuntenbrief auteursrecht 20©20 van 11 april 2011, p. 9.
[96] Zie daarover par. 3.3.

wettelijke waarborgen die ervoor zorgen dat rechthebbenden geen afgifte van persoonsgegevens kunnen afdwingen van consumenten die op beperkte schaal up- en downloaden. Afgifte mag alleen aan de orde zijn als de rechter heeft vastgesteld dat iemand zich schuldig heeft gemaakt aan grootschalige auteursrechtinbreuken en als het niet mogelijk is gebleken om de websitebeheerder of de hosting provider effectief aan te spreken'.[97]

Het is de vraag wat dit uitgangspunt voor watermerken betekent. De inzet van watermerken heeft naar zijn aard geen zin meer wanneer iemand enkel zou kunnen worden aangesproken als de rechter heeft vastgesteld dat iemand zich schuldig heeft gemaakt aan grootschalige auteursrechtinbreuken. Hoewel het niet duidelijk wordt uit de hiervoor geciteerde tekst lijkt het te gaan om de situatie waarin derden in het bezit zijn van de gewenste persoonsgegevens. In het laatste deel verwijst het kabinet immers naar de onmogelijkheid om een derde effectief aan te spreken. Niet duidelijk is wat dit betekent voor situaties, zoals bij watermerken, waarbij in beginsel geen derde hoeft te worden aangesproken omdat de gegevens reeds in het bezit zijn van de rechthebbende.[98] Het gaat dan niet langer om de afgifte bij een derde maar om specifieke waarborgen die ervoor moeten zorgen dat rechthebbenden geen afgifte van persoonsgegevens kunnen afdwingen van consumenten die op beperkte schaal up- en downloaden. Met andere woorden mag je nog persoonsgegevens in een watermerk opnemen nu het bij individuele watermerken per definitie onduidelijk is of de licentienemer dit op grote schaal doet? Het probleem is dat het kabinet niet wil handhaven bij consumenten die op beperkte schaal bestanden up- en downloaden en hiervoor als middel de beperking van de afgifte van persoonsgegevens inzet waardoor de civielrechtelijke handhaving in de praktijk lastiger wordt. Het doel is om consumenten die op beperkte schaal up- en downloaden niet langer aan te spreken. Om te voorkomen dat dit wel mogelijk is via het civielrecht wordt de opsporing daarvan bemoeilijkt. In dat kader is het niet ondenkbaar dat het kabinet watermerken onwenselijk vindt.[99] Deze regeling geldt vanwege de beperking tot up- en downloaden niet voor andere e-diensten waarvoor afgifte van persoonsgegevens noodzakelijk is, zoals voor het fysiek afleveren van boeken. Voor watermerken zou dit overigens vooral als consequentie hebben dat er na de vaststelling van inbreuk door de rechthebbende toestemming van de rechter nodig zou zijn voor het uitlezen van het watermerk. Dat het kabinet zelf niet wil handhaven bij consumenten die op beperkte schaal bestanden up- en downloaden kan ik begrijpen. De overheid moet in het kader van het strafrecht immers prioriteiten stellen en laat om die reden de handhaving van intellectuele eigendomsrechten over aan de rechthebbende. Het lijkt mij vanuit het systeem van de wet, dat zowel up- als downloaden in beginsel verbiedt, onjuist om niet te willen handhaven bij consumenten die op beperkte schaal bestanden up- en downloaden. Voor het op beperkte schaal downloaden zijn, in het licht van

[97] Speerpuntenbrief auteursrecht 20©20 van 11 april 2011, p. 9. Tot op heden is er nog geen wetgeving of jurisprudentie die in deze richting wijst.
[98] De door de TTP verwerkte persoonsgegevens zijn bedoeld voor zijn klanten. De rechthebbende is als klant van de TTP dan ook geen derde.
[99] Een dergelijke regeling heeft voor de consument wel als voordeel dat hij dan beschermd zou zijn tegen een zogenoemde lockin die nu ontstaat omdat de goedwillende consument niet anders kan dan zijn persoonsgegevens af staan in ruil voor toegang tot de werken van de rechthebbenden.

de verschillende onderzoeken, voldoende argumenten aan te voeren om het handhaven daarvan op een laag pitje te zetten.[100] Ook de entertainmentindustrie richt zich niet (meer) op downloaders. Voor het niet optreden tegen uploaders zie ik echter geen ruimte. Bij het uploaden van auteursrechtelijk beschermde werken lijkt mij ook niet van belang of iemand dat op grote of op kleine schaal doet. Iedere upload geeft immers onmiddellijk voor meer personen toegang tot die werken waardoor de rechthebbende zelf geen tegenprestatie meer kan vragen voor zijn werk. Het bemoeilijken van de handhaving lijkt mij dan ook geen weg die in dit geval bewandeld moet worden. De hier bedoelde wetgeving lijkt mij dan ook terecht (nog) niet ingediend.

In Nederland geldt samenvattend van overheidswege een voorkeur voor civielrechtelijke handhaving, waarbij het strafrecht een ultimum remedium is.[101] Samenwerking tussen het OM en civiele partijen is niet ondenkbaar. Al heeft het OM daarbij wel de zelfstandige plicht de aanwijzingen van College van procureurs-generaal te volgen.[102] Zie in dat verband ook de uitspraak van het Hof ’s-Gravenhage dat het OM niet-ontvankelijk achtte in een zaak tegen een zevental verdachten rond twee websites.[103] In deze zaak had het OM zijn vervolgingsbeslissing ten onrechte enkel gebaseerd op de dossiers van stichting Brein zonder zelf een nader onderzoek te verrichten. Mede op grond van de in de Aanwijzing Intellectuele Eigendomsfraude vermelde criteria voor strafrechtelijke handhaving, had het OM volgens het hof niet in redelijkheid tot zijn vervolgingsbeslissing kunnen komen, waardoor het OM de beginselen van een behoorlijke procesorde heeft geschonden. De strafrechtelijke handhaving van het auteursrecht is door deze aanwijzing zeer beperkt geworden.

3.3.1.3 België

In België is er geen specifiek beleid voor het handhaven van het auteursrecht. In tegenstelling tot Nederland is er vanuit de Belgische overheid ook veel minder aandacht besteed aan handhavingsproblemen rondom het auteursrecht. Inhoudelijk lijken de Nederlandse en Belgische regering overigens niet te verschillen in de visie op de wijze waarop rechthebbenden zelf met oplossingen kunnen komen. Zo gaf ook de (federale) minister in België in antwoord op een schriftelijke vraag vanuit de senaat aan dat hij naast het (Europees) wettelijk kader ook een rol voor de sector zelf ziet door enerzijds een samenwerking tussen rechthebbenden en service providers en anderzijds door het realiseren van voldoende attractief

[100] Zie o.m. Leenheer e.a. 2012 die erop wijzen dat ‘wie actief bezig is met muziek, films en series, games of boeken, meer zal downloaden uit illegale bron, maar zal ook meer legaal consumeren en meer afgeleide producten afnemen’ Zie verder par. 3.2.2.
[101] Spoor/Verkade/Visser 2005, p. 533 achten dit een terecht uitgangspunt.
[102] Aanwijzing intellectuele-eigendomsfraude (2005A022) van het College van procureurs-generaal, Stc. 9 januari 2006, nr. 6, pag. 10 (laatstelijk verlengd tot 31-01-2016; Stc 2010, nr. 1021)
[103] Hof ‘s-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010 (e-Donkey indexeringsites), m.nt. Duker. De Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 had eerder geen problemen met een vervolging door het OM.

legaal aanbod.[104] Ten aanzien van de handhaving van het auteursrecht verwijst hij naar Europese ontwikkelingen en wijst hij op de complexiteit van het fenomeen van illegaal downloaden dat volgens hem tot uiting komt in de grote diversiteit aan voorstellen en het gebrek aan betrouwbare cijfers over de economische impact van namaak en piraterij. Ook voor België geldt dat sinds de uitspraak van het HvJ EU inzake ACI Adam/Stichting Thuiskopie er sprake is van een downloadverbod.[105]

De Belgische auteurswet vormt evenals in Nederland het uitgangspunt ten aanzien van de civiele en strafrechtelijke handhavingsmogelijkheden.[106] In België wordt de handhaving van het auteursrecht als een probleem van openbare orde gezien waardoor de inzet van het strafrecht ook in de praktijk mogelijk wordt. Het strafrecht en met name de verhoging van straffen in 2007 komt ook voort uit de gedachte dat handhaving een afschrikkend karakter moet hebben in gevallen van namaak en piraterij op grote schaal, en gediversifieerd moet zijn in het licht van de nieuwe ontwikkelingen.[107] Het Openbaar Ministerie (hierna: OM) kan ambtshalve optreden tegen auteursrechtinbreuk omdat de namaking in het auteursrecht als een verstoring of aantasting van de (economische) openbare orde wordt beschouwd.[108] Daarnaast kan de rechthebbende zelf een klacht bij het OM indienen of een klacht met burgerlijke partijstelling indienen bij de onderzoeksrechter.[109] De benadeelde partij kan zich tot het sluiten van de debatten als burgerlijke partij stellen.[110] Het staat de benadeelde vrij alle schade die voortvloeit uit het betrokken misdrijf te vorderen, maar het is aan de rechter om deze te begroten.[111] Het voordeel van de strafrechtelijke route is voor de rechthebbende vooral dat hij de zaak verder aan het OM kan laten. Hij is dan zelf geen proceskosten en kosten voor onderzoeksmaatregelen verschuldigd. Daar staat tegenover dat de procedures langer duren.[112] Bij een vrijspraak zal de rechter zich echter onbevoegd verklaren ten aanzien van de civiele vordering. In de praktijk ligt de prioriteit voor het opsporen en aanpakken van

[104] In antwoord (29-04-2011) op de schriftelijke vraag nr. 5-1597 van Bert Anciaux (sp.a) d.d. 2 maart 2011; zie ook de schriftelijke vraag en het antwoord 0238 door Destrebecq als minister van Economie, Consumenten en Noordzee (18-03-2013).
[105] HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie).
[106] Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, B.S., 27 juli 1994, in werking getreden op 1 augustus 1994. De wet is daarna vooral door de omzetting van diverse Verdragen en Europese Richtlijnen verschillende malen gewijzigd (Zie o.m. Werkers e.a. 2009, p. 10).
[107] MvT (DOC 51 2852/001), p. 4, 17.
[108] Parl. Stukken Kamer, Doc. 51-2852/1, p. 35. De gedachte daarachter is dat deze inbreuken de grondslag van de (kennis)economie aantasten, steeds vaker banden heeft met georganiseerde criminaliteit en de overheid (belasting)inkomsten misloopt (Van Damme 2009).
[109] Een van de belangrijke verschillen in beide benaderingen is dat in het eerste geval het OM de zaak kan seponeren en in het tweede geval de onderzoeksrechter de zaak niet kan seponeren maar de Raadkamer of Kamer van inbeschuldigingsstelling een oordeel zal moeten uitspreken. Daarbij moet worden opgemerkt dat de beslissing over de strafvordering wordt opgeschort tot er een in kracht van gewijsde gegane beslissing is genomen over de vordering tot staking. Zie artikel 80 Aw (art. 28 WNP) en ook wel bekend als het principe van 'Le civil tient le criminel en état'.
[110] Art. 67 Sv. Dit kan hij zowel voor de onderzoeksrechter, onderzoeksgerechten als voor de vonnisgerechten; Cass. 9 oktober 1990, A.C. 1990-91, 65.
[111] Verstraeten, 2012, p. 139-140; Cass. 23 februari 1994, A.C 1994, 91. Naast gederfde inkomsten worden ook bijkomende (en toekomstige) indirecte schade vergoed om te voorkomen dat misbruik wordt aangemoedigd wanneer enkel de gederfde inkomsten vergoed zouden hoeven worden. Maeyaert 2008, p. 454.
[112] Gotzen & Janssens 2009, p. 274.

auteursrechtinbreuk niet hoog en kan er derhalve gesproken worden van passieve handhaving van het auteursrecht.[113] In tegenstelling tot Nederland is het echter wel mogelijk om in de praktijk daadwerkelijk strafrechtelijk op te treden tegen inbreuk op het auteursrecht.[114]

De handhavingsmogelijkheden ten aanzien van internet gerelateerde inbreuken zijn in 2007 verruimd door de implementatie van de Handhavingsrichtlijn in drie bijzondere wetten. De wet van 9 mei 2007 betreffende de burgerrechtelijke aspecten van de bescherming van intellectuele eigendomsrechten en de wet van 10 mei 2007 betreffende de aspecten van gerechtelijk recht van de bescherming van intellectuele eigendomsrechten, op grond waarvan onder meer een stakingsbevel kan worden uitgesproken ten aanzien van tussenpersonen wier diensten worden gebruikt om inbreuk te plegen op het auteursrecht of naburige rechten. Op grond van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten (WNP) zijn naast het OM, politie, douaneambtenaren en door de minister aangewezen ambtenaren, ook daartoe aangestelde ambtenaren van de Algemene Directie Controle en Bemiddeling van de Federale Overheidsdienst Economie bevoegd om de (strafrechtelijke) op internet begane inbreuken op het intellectuele eigendomsrecht vast te stellen.[115] Deze met de controle op de namaak belaste diensten werken onder toezicht van het Parket-Generaal.[116] De door deze ambtenaren opgemaakte processen-verbaal hebben bewijskracht tot het tegendeel is bewezen. Om de opsporing en vaststelling te versterken kan er een maximale boete van € 2.000,- worden opgelegd aan hen die opdrachten van de eerder genoemde ambtenaren voor het opsporen en vaststellen van de inbreuken of het niet-naleven van deze wet, verhinderen of belemmeren.[117]

Een andere wijze waarop het beleid rondom de handhaving van het auteursrecht vorm krijgt is door publiek-private samenwerking. Nationale (auteursrecht)wetgeving wordt door de Dienst voor de Intellectuele Eigendom (DIE) als onderdeel van Federale Overheidsdienst (FOD) economie nader uitgewerkt. In 2012 heeft de FOD economie met de Belgian Anti-Piracy Federation (hierna: BAF) een samenwerkingsakkoord gesloten om de strijd tegen piraterij en namaak op internet op te voeren door de reeds bestaande middelen, technische mogelijkheden, kennis en de onderzoeksbevoegdheden zo goed mogelijk te benutten.[118] Deze

[113] Gesprekken met BAF.
[114] Onderzoek naar de vraag of strafrechtelijke handhaving leidt tot minder inbreuk op het auteursrecht dan bijvoorbeeld in Nederland onderbreekt. Het is op basis van eerder genoemde Frans, Noors en Zweeds onderzoek echter niet aannemelijk dat strafrechtelijk handhaving leidt tot minder inbreuk. Zweeds onderzoek wijst uit met name de handhavingscapaciteit ('pakkans') een belangrijke rol speelt bij het verminderen van auteursrechtelijke inbreuk. Zie Schermer & Wubben 2011.
[115] Art. 18 jº 20 WNP. Deze wet had ten doel de Vo 1383/2003 te implementeren en strafrechtelijke bepalingen te moderniseren waardoor er ook dacht is besteed aan de opsporing en vaststelling daarvan (Parl. Stukken, Doc 2852/1, p. 3-4).
[116] De minister merkt op dat in dit verband verschillende samenwerkingsverbanden zijn opgericht die, onder de leiding van de parketten, tot gezamenlijke acties hebben geleid. Dit in antwoord (29-04-2011) op de schriftelijke vraag (nr. 5-1597) van Bert Anciaux (sp.a) d.d. 2 maart 2011.
[117] Artikel 11 Wet van 2007. Dit kan enkel worden toegepast in administratief onderzoek dat vooraf gaat aan een strafrechtelijke vervolging omdat in het strafonderzoek (opsporing en gerechtelijk onderzoek) andere rechten zoals het zwijgrecht en het verbod van zelfincriminiatie een rol spelen.
[118] Zie persbericht FOD economie op 17 oktober 2012.

samenwerking moet leiden tot een groter legaal aanbod, het versterken van consumentenvertrouwen in legaal onlineaanbod en betere bescherming van de intellectuele-eigendomsrechten van artiesten, producenten en andere rechthebbenden.

In België bestaan de civiele en strafrechtelijke handhaving zowel wettelijk als in de praktijk naast elkaar. Vanuit die gedachte is het ook in België mogelijk dat de onderzoekersrechter als voorlopige strafrechtelijke dwangmaatregel aan internettoegangleveranciers het bevel kan geven om 'de toegang ontoegankelijk te maken tot de inhoud die wordt gehost door de server gekoppeld aan de hoofddomeinnaam 'thepiratebay.org'.[119] Een mogelijke verklaring voor de relatieve afwezigheid van het auteursrechtdebat in de politiek kan gevonden in de situatie dat in België veel beleidsruimte reeds gebruikt wordt. In de auteurswet zijn zowel civiel als strafrechtelijke sancties opgenomen en deze worden in de praktijk ook ingezet. Daarnaast is gebruik gemaakt van publiek-private samenwerking tussen de FOD economie en bijvoorbeeld BAF. Behoudens andere wetgeving zijn hiermee alle gebruikelijke beleidsinstrumenten gebruikt.

3.3.2 Particulier handhavingsbeleid

Het idee om alle onrechtmatige content eeuwig van het internet te weren wordt in het algemeen als onhaalbaar gezien. File-sharing en downloaden zijn een onderdeel geworden van het dagelijks internetgebruik.[120] Rechthebbenden richten zich nu vooral op een goed legaal aanbod en in termen van handhaving op het vertragen van het distributieproces van illegale werken. De handhavingstrategie ziet dan vooral op het aanpakken van de 'grote' uploaders en het verhinderen van de 'eenvoudige toegang' tot deze content. In de praktijk betekent dit dat uploaders juridisch worden vervolgd en dat filesharingwebsites zoals Mininova en Pirate Bay juridisch worden aangepakt, waar mogelijk.[121] Daarnaast kan de toegang ook worden beperkt doordat bijvoorbeeld internetzoekmachines zoals Google de

http://statbel.fgov.be/nl/modules/pressrelease/s4/20121017_lutte_contre_piraterie_et_contrefacon_intensifie.jsp Eerder was Bij de Algemene Directie Controle en Bemiddeling is er een specifieke cel opgericht die belast is met de controle op de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten.

[119] Art. 39bis onder 4 Sv. Cass. 22 oktober 2013, P.13.0550.N (Telenet, Tecteo en Brutele), dit met het oog op de waarheidsvinding, de verbeurdverklaring, de teruggave, het doen ophouden van handelingen die een misdrijf lijken uit te maken of ter beveiliging van civielrechtelijke belangen' (ov. 8). De maatregelen via de civiele weg (Hof van Beroep Antwerpen, 26 september 2011, RABG 2011/18, 1269) waren eerder onvoldoende effectief gebleken, omdat The Pirate Bay o.m. via de nieuwe domeinnaam depiraatbaai.be. bereikbaar bleef. Dit lijkt in lijn met HvJ EU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien).

[120] Zie ook Hugenholtz 2012; Huygen e.a. 2009 (p. 136) die concluderen dat 'file sharing niet meer zal verdwijnen en dat downloaders tevens belangrijke klanten zijn van de muziekindustrie. Het 'point of no returm' is gepasseerd. en het is onaannemelijk dat de geest weer terug in de fles gaat. Daarnaast is ook niet gegarandeerd dat er ooit sprake zal zijn van een situatie waarin het merendeel van de digitale downloads afkomstig is uit geautoriseerde bron.'

[121] Zie in Nederland o.m. Rb. 's-Gravenhage 11 januari 2012, ECLI:NL:RBSGR:2012:BV0549 (BREIN/Ziggo enX S4All); Hof Den Haag 28 januari 2014, ECLI:NL:GHDHA:2014:88 (Ziggo, XS4All/Stichting BREIN) en in België werd Rb. Koophandel Antwerpen 8 juli 2010, A/10/5374, IEF 10292 (BAF tegen Telenet/Belgacom) de vordering nog afgewezen. In hoger beroep echter toegewezen.

zoekresultaten aanpassen.[122] Daarnaast weert ook YouTube met behulp van algoritmen automatisch video's in het kader van Amerikaanse auteurswetgeving (DMCA).[123] Samenvattend wordt het probleem van downloaden gevormd door het beschikbaar komen van het materiaal en het eenvoudige kopieer- en distributiesysteem via het internet. Daarbij geldt dat één goede bron voldoende is om het aanbod aantrekkelijk te maken en dat de uploaders die deze content beschikbaar stellen over voldoende kennis en kennissen beschikken om dit mogelijk te maken.

3.3.2.1 Nederland

In Nederland kunnen drie typen particuliere handhavers worden onderscheiden. Ten eerste zij die als belangenorganisatie georganiseerd zijn en collectief voor of namens rechthebbenden handhaven, zoals Brein of Pictoright.[124] Ten tweede is er een groep organisaties die auteursrechten handhaven als dienstverlening voor (individuele) rechthebbenden, zoals Auxen of Getty Images.[125] Zij treden zowel op voor grote opdrachtgevers als voor individuen. Ten derde is er de individuele auteursrechthebbende zelf. Al deze typen handhavers maken per geval hun eigen afweging. In het algemeen zijn (de klanten van) de eerste twee groepen beleidsmatig van mening dat handhaving zich niet moet richten op individuele consumenten die content downloaden maar op personen die op grote schaal content uploaden of verspreiden en hiermee winst maken.[126] In dat licht is het opvallend dat Brein heeft aangegeven dat een groot aantal aanbieders van e-boeks contractueel verplicht wordt om op hun verzoek informatie van klanten door te spelen.[127]
Brein stelt daartoe dat het handhavend zal optreden als de omstandigheden dat rechtvaardigen. Zij geven op Tweakers als voorbeeld dat zij zich kunnen voorstellen dat zij de gegevens van de koper willen hebben wanneer een e-boek met watermerk kort na publicatie op internet verschijnt.[128] Brein herhaalt dat zij zich met de handhaving nog steeds niet richten op individuele uploaders, maar wel geïnteresseerd is in de vraag wie de uploader is omdat zij de bron is voor websites die deze werken aanbieden. Daaruit mag worden opgemaakt dat Brein onder omstandigheden wel van plan is individuele uploaders van e-boeken aan te gaan

[122] Zo kondigde google in 2012 aan de zoekresultaten mede afhankelijk worden van de mate waarin een website beschermd materiaal heeft moeten verwijderen. Hoe vaker, hoe lager de website in de resultaten verschijnt. http://insidesearch.blogspot.nl/2012/08/an-update-to-our-search-algorithms.html;
http://www.guardian.co.uk/technology/2012/aug/10/google-algorithm-hollywood-lobbyists-copyright;
[123] Door wired aangeduid als de Algorithmic Copyright Cops.
http://www.wired.com/threatlevel/2012/09/youtube-flags-democrats-convention-video-on-copyright-grounds/
[124] BREIN rondde vorig jaar 651 onderzoeken af naar illegale handel in ongeautoriseerde bestanden en kopieën van muziek, film, TV series, boeken en games. Daarbij werden 571 sites offline gehaald (en 1 geblokkeerd). Het ging hierbij om file-sharing sites, streaming en downloadsites die volgens BREIN structureel toegang geven tot ongeautoriseerde bestanden.
[125] Zie ook Sandvliet & Engelfriet 2012, p. 204.
[126] Interviews met BREIN en Auxen. Voor België met BAF. Zie ook verklaringen in media, waar Brein opmerkt dat het ook kan gaan om een individuele uploader van een film. http://www.anti-piracy.nl/artikelen.php?id=18;
[127] http://tweakers.net/nieuws/90880/brein-e-book-aanbieders-gaan-klantinformatie-doorspelen-bij-piraterij.html
[128] Idem.

pakken. Of en hoe dat in de praktijk gaat werken moet nog blijken.[129] Van een beleid bij de groep van individuele belanghebbenden kan niet worden gesproken. De individuele rechthebbende kan er per geval en om verschillende redenen voor kiezen om over te gaan tot handhaving van zijn recht.

Hoewel er weinig onderzoek is gedaan naar de motieven en handhavingsstrategieën van individuele rechthebbenden ontstaat wel het beeld dat de rechthebbende tot handhaving over gaat om principiële redenen (het is mijn recht en niet dat van jou) of vanwege de derving van inkomsten.[130] In dit laatste geval speelt ook een rol of de rechthebbende in staat is om op andere wijze inkomsten te verkrijgen. Van een algemeen beleid inzake auteursrechtinbreuk kan, mede vanwege de verschillen per type handhaver, branche en content, echter niet worden gesproken.[131] De handhavingsbehoefte van rechthebbenden lijkt sterk samen te hangen met de vraag of de rechthebbende op een alternatieve manier aan zijn inkomsten kan komen.[132]

De wijze waarop de handhaving plaatsvindt hangt mede samen met de opsporingscapaciteit die de rechthebbenden ter beschikking hebben. De eerste twee categorieën rechthebbenden hebben vanwege hun omvang en specifieke aard meer en betere middelen ter beschikking dan de individuele rechthebbende. Dit komt tot uiting in zowel de opsporingsmogelijkheden, bijvoorbeeld door het laten draaien van meerdere en betere webcrawlers als in de mate waarin jurdische actie kan worden ondernomen.[133] Organisaties die primair met de handhaving zijn belast, zoals Brein of Buma/Stemra hebben naast technische mogelijkheden vaak ook juridisch een grotere slagkracht terwijl de individuele rechthebbende vanwege de kosten zich vaak genoodzaakt ziet eerst zelf een brief te schrijven.

Het beeld van de handhaving wordt niet zelden bepaald door zaken waarbij een groot gevoel van onrecht overheerst, zoals in de zaak van een 15-jarige jongen die via google een foto van Johan Cruijff had gevonden en op zijn website soccer4you.nl had geplaatst waar hij nieuws over voetbal verzamelde. De fotograaf voerde een procedure waarin de jongen werd

[129] Op 21 oktober 2014 meldde het NUV aan mij dat men tot op heden nog geen rechtszaken zijn gevoerd tegen natuurlijke personen of rechtspersonen waarbij het watermerk een rol speelde. En dat zij ook niet op de hoogte waren dat er een schikking was getroffen.

[130] Zie o.m. de conclusies van Weda e.a. 2011, p. 87. Vanzelfsprekend kunnen meerdere motieven een rol spelen.

[131] Onder makers of creatieven is geen overeenstemming over de vraag hoe er met filesharing moet worden omgegaan. Een (kleine) meerderheid is van mening dat er harder moet worden opgetreden tegen consumenten en websites. Deze groep staat positief tegenover de inzet van technische (gebruiks)beperkingen. Weda e.a. (2011, p. i en 87) geven aan dat cijfers over 'voor' of 'tegen' geen recht doen 'aan de verscheidenheid aan opinies die daaronder verscholen ligt'.

[132] Zo maakte de band Iron Maiden in 2013 bekend een tour te plannen rondom de locatie van bittorrentgebruikers. http://www.nu.nl/tech/3662081/iron-maiden-plant-tour-basis-van-locatie-bittorrent-downloaders.html

[133] Veel organisaties maken gebruik van zogenaamde webcrawlers. Deze techniek stelt hen in staat audio en video die op internet geplaatst is op te sporen. De grote belangenorganisaties hebben inmiddels met onder andere YouTube afspraken gemaakt om door middel van fingerprinting vooraf materiaal te detecteren op evidente inbreuk. Bij het signaleren van auteursrechtelijk materiaal krijgt de rechthebbende een bericht van YouTube en kunnen zij bepalen welk vervolg zij daaraan willen geven. Zie ook Gerkens 2009, p. 23.

veroordeeld tot de betaling van een schadevergoeding en proceskosten van in totaal € 4000.[134] Deze zaken halen het nieuws, maar komen in de praktijk niet heel vaak voor.[135] Zaken die het nieuws halen zijn bovendien veelal gebaseerd op zaken in Verenigde Staten.[136] De keuze van deze individuele fotograaf, lijkt niet representatief voor deze wijze waarop de verschillende groepen rechthebbende tegen handhaving van het auteursrecht aankijken.[137] In het algemeen lijkt er onder makers voornamelijk consensus over de aanpak van het grootschalige illegale aanbod en dan met name ten aanzien van mensen die daar geld aan verdienen zonder een deel daarvan aan de makers te geven.[138] Dit sluit aan bij de wens van het kabinet en de praktijk van (de klanten van) grote (handhavings)organisaties om geen individuele gebruikers te vervolgen maar zich te richten op de groep die winst maakt door onrechtmatig werken aan te bieden en te verspreiden.[139] Maar hiermee is natuurlijk niet gezegd dat individuele personen niet op inbreuk kunnen worden aangesproken en dat het achterwege blijven van de gewenste gedragsverandering niet tot juridische sancties kan leiden.
Rechthebbenden die watermerken willen inzetten zullen zich moeten realiseren dat het preventieve effect van watermerken op termijn alleen blijft bestaan wanneer er ook gehandhaafd wordt, al is het maar symbolisch. Zonder daadwerkelijke handhaving neemt de eerder genoemde dreiging van (juridische) sancties immers af.

3.3.2.2 België

Ook in België kunnen drie typen particuliere handhavers worden onderscheiden die kunnen worden onderverdeeld in grote collectieve belangenorganisaties (Sabam, BAF) en

[134] Rb. 's-Hertogenbosch 2 oktober 2008, ECLI:NL:RBSHE:2008:BF9979. Zie voor kritiek op deze zaak o.m. Engelfriet (AE 1294). Zie ook Rb. Haarlem 19 november 2008, ECLI:NL:RBHAA:2008:BG5139, waarin gedaagde op zijn website een door een beroepsfotograaf gemaakte foto van Johan Cruijff heeft geplaatst.
[135] De zoektermen [auteursrecht, uploaden] gaf op 30 december 2014 in het rechtsgebied civiel recht op rechtspraak.nl 30 resultaten. Van de 30 zaken is dit de enige zaak waarbij een particulier wordt gedagvaard vanwege het uploaden van content. In een andere zaak waarin een particulier tegen Brein optrad ging het om het faciliteren van inbreuk en hield de rechter bij het toewijzen van de proceskosten rekening er onder meer rekening mee dat het in ontwikkeling zijnde materie betrof, waarbij een professionele belangenorganisatie staat tegenover een thuiswonende student die zich als hobby bezig hield met het ontwikkelen van de in geding zijnde site (Hof Amsterdam 2010, 16 maart 2010 BL7920, IER 2010, 78 inzake ShareConnector)
[136] Sinds 2008 heeft RIAA in de VS de handhavingsstrategie van het vervolgen individuele downloaders officieel verlaten maar lopende zaken zijn voortgezet (Slattery 2008). Hier kon recent Joel Tenenbaum nog worden veroordeeld voor het downloaden van 31 muziekbestanden (na eerder verschillende schikkingsvoorstellen van o.a. $ 5.250 te hebben geweigerd) tot betaling van een schadevergoeding van $ 675.000 (US District Court of Massachusetts, No. 07-111446-RWZSONY (BMG Music Entertainment/Joel Tenenbaum), August 23, 2012).
[137] De zoektermen [auteursrecht, uploaden] gaf op 30 december 2014 in het rechtsgebied civiel recht op rechtspraak.nl 30 resultaten. Van de 30 zaken treden de grote entertainmentbedrijven veelal verenigd in Brein, enkel op tegen website die inbreuk faciliteren en niet één keer tegen een particulier. Hiermee is overigens niet gezegd dat dit niet voorkomt of dat er geen (al dan niet terecht) sommatie worden verstuurd naar particulieren.
[138] In het onderzoek van Weda e.a. 2011 (p. 30) gaven respondenten aan niet van alle gebruikers een vergoeding te willen ontvangen. Zo gaf ruim 60 procent aan geen vergoeding te hoeven ontvangen van ideële organisaties. Voor gebruik door onderwijs, bibliotheken, musea en archieven hoefde 40 procent van hen geen vergoeding te ontvangen.
[139] Zie in dat kader ook het plan van de Europese Commissie (1 juli 2014, Memo 14/449; persbericht IP/14/760) waarin zij nieuw handhavingsbeleid aankondigt ten aanzien van IP en daarbij expliciet o.m. als voorbeeld noemt: 'the so-called "follow the money" approach which aims to deprive commercial scale infringers of their revenue flows.

organisaties die de handhaving van auteursrecht als dienst aanbieden voor (individuele) rechthebbenden. Zij treden zowel op voor grote opdrachtgevers als voor individuen. Als derde kunnen ook individuele rechthebbenden zelf optreden tegen inbreuk op hun auteursrecht. De eerste categorie betreft vooral de grote collectieve belangenorganisaties. Zij kiezen er evenals in Nederland voor om niet de individuele downloader aan te pakken maar degene die bestanden verspreiden.[140] Daarmee is echter niet uitgesloten dat individuele uploaders van bijvoorbeeld nieuwe films worden aangepakt. De prioriteit van de opsporing ligt hier echter evenals in Nederland niet.[141]

Doordat de inzet van het strafrecht in België tot de mogelijkheden behoort, zijn het vooral de grote partijen, zoals BAF die de handhavingspraktijk vorm geven door zelf bewijs te verzamelen en dit daarna over te dragen aan de politie voor verdere opsporing. Door goede (bewijsbare) dossiers te overhandigen is het aantrekkelijk voor de politie om deze zaken op te pakken. De zelfregulering is daarbij gegeven omdat beide partijen alleen zaken kunnen doen als de dossiers goed zijn. Met name collectieve organisaties die gelden als repeatplayer zijn er bij gebaat om adequate keuzes te maken en alleen die zaken aan te leveren die voldoende bewijsbaar zijn. Op die manier slagen belangenorganisaties er in België in om bepaalde zaken via het strafrecht af te doen.

3.3.3 Tussenconclusie

Om te kunnen beoordelen of het watermerk een effectief juridisch bewijsmiddel kan vormen bij de handhaving van inbreuk op auteursrecht op digitaal beschikbaar gestelde werken op internet, is in deze paragraaf aandacht besteed aan de vraag of het watermerk past in het handhavingsbeleid van zowel de overheid als particulieren. Nationale wetgevers hebben vanwege de vergaande mate waarin het auteursrecht is geharmoniseerd door de verschillende Europese richtlijnen, een beperkte beleidsruimte voor het vinden van oplossingen voor de problemen waarvoor het internet het auteursrecht heeft geplaatst.

Nederland en België hebben allebei civiel- en strafrechtelijke sancties opgenomen in hun nationale auteurswet. Nederland heeft in tegenstelling tot België duidelijk de voorkeur voor civiele handhaving en heeft strafrechtelijke handhaving in de praktijk lastig uitvoerbaar gemaakt. Voor beide landen geldt dat het watermerk zal worden ingezet door civiele partijen. In het strafrecht zal het watermerk enkel als bewijs dienen in het geval een civiele partij het als bewijs aan strafrechtelijke opsporingsinstanties overhandigt. In tegenstelling tot Nederland is het gebruik van het watermerk in België als strafrechtelijk bewijs niet ondenkbaar vanwege de mogelijkheid voor rechthebbenden om aangifte te doen. Weliswaar is aangifte in Nederland ook mogelijk maar leidt dat in de praktijk nauwelijks tot vervolging. Zowel de nationale wetgeving als het nationale beleid inzake de handhaving van het auteursrecht staat

[140] Zie ook http://datanews.knack.be/ict/nieuws/baf-geen-klacht-tegen-downloaders-wel-tegen-verspreiders/article-4000614957951.htm (2014).
[141] Onder meer opgemaakt uit gesprekken met BAF.

in beide landen derhalve niet in de weg aan het beoogde gebruik van watermerken door civiele partijen.

De volgende vraag is dan of het watermerk aansluit bij de wijze waarop particuliere organisaties het auteursrecht handhaven. Duidelijk is geworden dat (de klanten van) grote belangenorganisaties zich in beginsel niet richten op individuele uploaders, zolang deze de werken niet op grote schaal verspreiden en hier geen winst mee behalen. Hiermee is niet gezegd dat deze groep helemaal niet wordt aangepakt, maar enkel dat het geen prioriteit heeft om deze groep juridisch aan te spreken. In dat kader is het opmerkelijk dat uitgeverijen die e-boeken voorzien van een watermerk voornemens zijn om mensen die deze boeken op downloadsites aanbieden actief op te sporen. Om die reden is al in 2010 een samenwerkingsovereenkomst gesloten tussen de Nederlandse Uitgeversbond en Stichting Brein. Bij individuele rechthebbende is geen eenduidig beleid waarneembaar. De individuele rechthebbende maakt zijn eigen afweging waardoor het mogelijk is dat de ene rechthebbende wel en de andere niet besluit om achter een individu aan te gaan.

Van overheidswege is het in beide landen aan de rechthebbende gelaten om technieken, zoals watermerken in te zetten voor de handhaving van het auteursrecht. Inmiddels is duidelijk dat watermerken worden ingezet bij e-boeken. Hiermee lijken grote belangenorganisaties in ieder geval niet principieel tegen het handhaven van individuele uploaders te zijn. Of dat beleid, na het downloadverbod, ook gaat gelden voor downloaders is op dit moment nog onduidelijk.[142] Of watermerken ook in meer sectoren zal worden toegepast hangt af van de kosten van de techniek en het bijbehorende verdienmodel vanuit de ondernemingen die een watermerkservice leveren. Bij lage kosten per transactie kan de techniek mogelijk ook interessant zijn voor individuele rechthebbenden die in beginsel zelf de afweging maken of zij tot handhaving over willen gaan. De rechthebbende kan dat doen ter preventie of met als doel de uploaders daadwerkelijk te gaan opsporen en aan te spreken. Met de inzet van watermerken kan de rechthebbende de keuze of hij wil handhaven ook uitstellen. Hij heeft met de inzet ervan in ieder geval de mogelijkheid de licentienemer op te sporen.

Vanwege de (juridische) handhavingskosten zal het watermerk als eerste een preventieve functie moeten hebben. Hiervoor is het noodzakelijk dat de rechthebbende duidelijk aangeeft dat de producten zijn voorzien van een onwaarneembaar watermerk. Daarbij moet worden opgemerkt zoals eerder in paragraaf 3.3.2 naar voren kwam dat het watermerk voornamelijk bedoeld is om een grote groep eerlijke gebruikers eerlijk te houden en dat daarvoor het watermerk voldoende robuust moet zijn om de kleine groep malafide aanvallers te weerstaan.

Al hoewel dit strikt genomen buiten de onderzoeksvraag valt, zal de handhaving van het auteursrecht ten aanzien van content naar mijn mening alleen succesvol kunnen zijn wanneer consumenten er van kunnen worden overtuigd dat het beter of aantrekkelijker is om voor

[142] Zie HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie); par. 3.3.1.2 en 3.3.1.3.

content te betalen dan dit gratis te downloaden. De consument overtuigen dat er legaal een voldoende en aantrekkelijk aanbod is, is iets anders dan de stelling van Stichting BREIN dat er legaal aanbod is.[143] Het zal niet eenvoudig zijn om de consument te overtuigen want tegen gratis valt lastig te concurreren. De meest aannemelijke weg lijkt mij om het legale aanbod te vergroten en het illegale aanbod zo klein mogelijk te houden. Dat kan alleen als de grote rechthebbenden zich verenigen en er uiteindelijk een markt komt waarin de consument bij twee of drie distributiekanalen snel de laatste content kan bekijken of beluisteren. Als de consument bij verschillende platformen moet zoeken naar de content die hij wenst dan kan hij vanuit zijn perspectief beter gratis downloaden. De toekomst zal uitwijzen of rechthebbenden er in voldoende mate in slagen om een aantrekkelijk legaal aanbod te presenteren. Daarbij is het niet ondenkbaar dat bepaalde rechthebbenden ook op zoek gaan naar alternatieve manieren om geld te verdienen, om op die manier in combinatie met een goed aanbod tot voldoende middelen te komen om content te blijven produceren. De wensen en mogelijkheden zullen per branche en mogelijk zelfs per rechthebbende verschillen. Zo zullen rechthebbenden in de muziek- en filmmarkt mogelijk op een eenvoudigere wijze extra inkomsten kunnen verwerven dan de markt voor e-boeken.
Zolang wij er niet voor kiezen om alles vrij te laten en de rechthebbende uit algemene middelen (bv. cultuurbelasting) te betalen moet de consument betalen voor de content. In deze benadering lijkt het downloadverbod mij de juiste weg. Het uitgangspunt en de norm moet dan zijn dat legaal gebruik de norm is en je moet betalen voor content.[144] Ook een ‘follow the money’ benadering, zoals door de Europese Commissie is genoemd lijkt mij een stap in de goede richting. Onderzoeken wijzen immers uit dat er weinig altruïsten zijn onder de uploaders. In de meeste gevallen gaat het, evenals bij de grote rechthebbenden gewoon om het verdienen van geld.

3.4 Watermerken en het probandum

De effectiviteit van het watermerk als juridisch bewijsmiddel wordt naast de hiervoor reeds genoemde elementen vooral bepaald door de rol die het krijgt in de context van het bewijsrecht. Zowel in Nederland als in België geldt dat op basis van het bewijsrecht en het materiële recht wordt bepaald welke rol het watermerk als juridisch bewijsmiddel kan spelen bij het vaststellen van auteursrechtinbreuk. Op die rol zal in deze paragraaf kort worden ingegaan aan de hand van de vraag wanneer er sprake is van inbreuk op het auteursrecht naar civiel (par. 3.4.1) en strafrecht (par. 3.4.2). De plaats van het watermerk in het bewijsrecht wordt verder behandeld in hoofdstuk 4.

De Nederlandse en Belgische auteurswet (hierna: Aw) geeft in overeenstemming met verdragen en Europese richtlijnen het uitsluitend recht om een werk te reproduceren, ter

[143] http://www.anti-piracy.nl/artikelen.php?id=21
[144] In dat licht zou de licentiestructuur ook opnieuw beoordeeld mogen worden. Het is vreemd dat iemand die in 1972 betaalt voor een licentie voor liedje van Elvis Presley op een LP, dat weer moet doen voor dezelfde muziek op een cassettebandje, later op een CD en nu voor bijvoorbeeld een mp3.

beschikking te stellen en mededeling daarvan te doen aan het publiek, aan de maker van een werk van letterkunde of kunst.[145] Naast de rechten voor de maker zijn er ook tal van beperkingen geformuleerd op zijn rechten, zoals het recht op privékopie en het citaatrecht.[146] Bij de aanschaf van content geeft de rechthebbende in de vorm van een licentie-overeenkomst toestemming voor de bepaalde gebruikshandelingen.[147] Bij consumenten is openbaarmaking op internet in de regel bij overeenkomst niet toegestaan en maken zij derhalve inbreuk op het auteursrecht wanneer zij de voorwaarden van de licentie-overeenkomst schenden.

Tot slot nog een opmerking over de verhouding tussen het nationale recht en het Europese recht. Hoewel de lidstaten in beginsel autonoom zijn in het invullen van algemene begrippen die niet nader zijn gedefinieerd in de Europese richtlijnen, benadrukt het Hof van Justitie EU dat deze begrippen geleidelijk vervangen zullen worden door een meer eenvormige unie-interpretatie.[148] Dat betekent dat in de toekomst steeds meer een gemeenschappelijke uitleg aan de begrippen wordt gegeven en de eventuele verschillen tussen beide in dit onderzoek betrokken landen zullen verdwijnen. De invulling en uitleg van de strafrechtelijke bepalingen blijft vooralsnog wel een exclusief recht van de lidstaten. Vanwege de vergelijking en omdat ook het bewijsrecht (nog) niet is geharmoniseerd in de EU is ervoor gekozen om ook voor het auteursrecht de benadering van beide lidstaten aan te houden.

3.4.1 Inbreuk op het auteursrecht als onrechtmatige daad

In de navolgende paragrafen wordt onderzocht wanneer er mogelijk sprake is van inbreuk op het auteursrecht naar Nederlands en naar Belgisch civiel recht.

3.4.1.1 Nederland

In Nederland is het auteursrecht voorbehouden aan de maker van een werk van letterkunde, wetenschap of kunst en is derhalve zijn uitsluitend recht, of van diens rechtverkrijgenden, om

[145] Zie o.m. art. 2 en 3 Auteursrechtrichtlijn; Richtlijn 2001/29/EG van 22 mei 2001 van het Europees Parlement en de Raad betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, PbEG L 167/10. Dit exclusieve recht is in beide landen geformuleerd in artikel 1 van Auteurswet. In Nederland in de Wet van 23 september 1912 en in België in de wet betreffende het auteursrecht en de naburige rechten van 30 juni 1994, gepubliceerd in het Belgisch Staatsblad (B.S.) ’op 27 juli 1994. Vgl. art. 9 BC.

[146] Zie artikel 5 van de Richtlijn en verder o.m. D.J.G. Visser, ‘De beperkingen in de Auteursrechtrichtlijn’, AMI 2001-1.

[147] Bij het downloaden of streamen van een film via bijvoorbeeld een Video On Demand service (VOD) ‘koopt’ de gebruiker de toestemming in de vorm van een licentie. Zie over licenties en de juridische koop, ook het commentaar van Quaedvlieg (2014) inzake het Usedsoft-arrest (3 juli 2012, zaak C-128/11).

[148] Zie voor het IE-recht (eerder HvJ EG 18 januari 1984, zaak 327/82, Jur. p. 107, ov. 11 inzake Ekro) o.m. de arresten van HvJ EU 16 juli 2009, C-5/08, Jur. p. I-6569, punt 27 (Infopaq); 21 oktober 2010, zaak C-467/08, ov. 31-37 (Padawan); 4 oktober 2011, zaken C-403/08 en C-429/08, ov. 154 en 185 (Premier League); 26 april 2012, zaak C-510/10, (DR en TV2 Danmark/NCB), ov. 33; 3 juli 2012, zaak C-128/11 (Usedsoft) ov. 39: ‘Volgens vaste rechtspraak vereisen de eenvormige toepassing van het Unierecht en het gelijkheidsbeginsel dat de bewoordingen van een bepaling van Unierecht die voor de betekenis en de draagwijdte ervan niet uitdrukkelijk naar het recht van de lidstaten verwijst, normaliter in de gehele Unie autonoom en uniform worden uitgelegd.’ Voor de hier bedoelde richtlijnen zie par. 3.3.1.1.

dit openbaar te maken en te verveelvoudigen, behoudens de beperkingen, bij de wet gesteld (art. 1 Aw). Er is met andere woorden sprake van inbreuk op het auteursrecht wanneer (1) een werk (2) openbaar is gemaakt of verveelvoudigd zonder dat degene die de handelingen verricht hiervoor toestemming heeft verkregen van de rechthebbende (licentie) of (3) een beroep kan doen op de zogenoemde wettelijke beperkingen.[149]

(1) Werk van rechthebbende moet auteursrechtelijk beschermd zijn

Om inbreuk op het auteursrecht te kunnen vaststellen zal eerst vastgesteld moeten worden of dat er sprake is van een auteursrechtelijk beschermd werk. Dat betekent dat het object van de eiser zelf voor bescherming in aanmerking moet komen. Het werkbegrip is in beginsel een nationaal begrip (art. 10 Aw), maar wordt in EU verband (art. 2 Rl. 2001/29/EG) inmiddels door het Hof van Justitie EU steeds vaker ingevuld.[150] In Nederland geldt dat er sprake is van een werk wanneer het object een eigen oorspronkelijk karakter heeft en het persoonlijk stempel van de maker draagt. '[D]at betekent dat sprake moet zijn van een vorm die het resultaat is van scheppende menselijke arbeid en dus van creatieve keuzes, en die aldus voortbrengsel is van de menselijke geest'.[151] Dit Nederlandse werkbegrip (EOK&PS) komt waarschijnlijk op hetzelfde neer als de uitleg van het Hof van Justitie EU dat stelt dat het werk oorspronkelijk moet zijn 'in die zin dat het gaat om een eigen intellectuele schepping van de auteur ervan' (EIS).[152] Wat het precies betekent, blijft ook in de praktijk lastig. Het betekent in ieder geval dat men het werk niet door (louter/integraal) kopiëren tot stand mag hebben gebracht.[153] En dat een zekere mate van creativiteit is vereist.[154] De vraag of een object auteursrechtelijk beschermd is betreft uiteindelijk een rechtsvraag die zich niet voor bewijslevering leent en waarover de rechter zich moet uitspreken.[155] Ook de Hoge Raad bemoeit zich daar bijvoorbeeld in het kader van de motiveringseis nauwelijks mee.[156] In dit onderzoek vormt het uitgangspunt dat de werken (muziek, films en foto's) die van een watermerk worden voorzien auteursrechtelijk beschermde werken zijn. Objecten watermerken

[149] Zie voor een meer inhoudelijke behandeling van het auteursrecht in het algemeen o.m. Spoor/Verkade/Visser 2005 en in het kader van software Struik, Van Schelven & Hoorneman 2010.
[150] Zie HvJ EU 16 juli 2009, C-5/08, NJ 2011/288 (Infopaq), HvJ EU 4 oktober 2011, C-403/08 en C-429/08, IEF 10286, (Premier League); HvJ EU 1 december 2011, zaak C-145/10 (Eva Maria Painer). De HR 25 oktober 2013, ECLI:NL:HR:2013:1036 (S&S/Esschert; Vuurkorven), ov. 4.1.2 erkent onder verwijzing naar het hiervoor genoemde Infopaq-arrest dat het werkbegrip inmiddels door het HvJ EU geharmoniseerd is.
[151] HR 30 mei 2008, ECLI:NL:HR:2008:BC2153, NJ 2008, 556 (Endstra/Nieuw Amsterdam; De Endstra Tapes), ov. 4.5.1.
[152] HvJ EU 16 juli 2009, C-5/08, Jur. p. I-6569, ov. 37 (Infopaq); herhaald in HvJ EU 4 oktober 2011, C-403/08 en C-429/08, IEF 10286, ov. 97 (Premier League).
[153] Zie o.m. Hugenholtz 1989 (diss.) 1989, p. 28; Visser 2004, p. 11.
[154] Visser 2004, p. 11.
[155] Spoor, Verkade & Visser 2005, p. 78. Partijen kunnen wel voldoende, concrete en relevante feiten aanleveren die als bewijs kunnen dienen voor stellingen over het werk, bijvoorbeeld dat het werk te weinig eigen karakter bezit omdat de gekozen vormgeving al gebruikelijk en daarom voor de hand liggend is. Visser (2004, p. 12) stelt ietwat badinerend dat iedere feitenrechter in de praktijk 'zelf mag weten wat hij wel en niet auteursrechtelijk beschermd acht' Visser 2004, p. 12.
[156] Zie o.m. HR 16 april 1997, NJ 1999, 697 m.nt. Hugenholtz (Bigott/Doucal). Zie ook Visser Motiveren in IE-zaken.

die zelf geen auteursrechtelijk beschermd werk vormen is in het kader van traitor tracing immers weinig zinvol.

(2) Werk moet openbaar zijn gemaakt of verveelvoudigd

Het openbaar maken en verveelvoudigen van auteursrechtelijk beschermde werken is behoudens de beperkingen bij wet gesteld, voorbehouden aan de rechthebbende en levert zonder diens voorafgaande toestemming dan ook inbreuk op het auteursrecht op.[157] Voor het uploaden van werken is met name het nationale begrip openbaar maken van belang. Voor inbreuk op het auteursrecht zal dan ook moeten worden vastgesteld dat er sprake is van openbaar making. Ook dit begrip moet worden uitgelegd in overeenstemming met het begrip 'mededeling aan het publiek' uit artikel 3 Auteursrechtrichtlijn.[158] Het plaatsen of uploaden van muziek, video of foto's op internet is eenvoudig te kwalificeren als een auteursrechtelijke openbaarmaking.[159] Naast de inhoud van het auteursrecht zijn er nog twee bijzondere rechten in de Auteurswet opgenomen. De maker komt een beroep toe op zijn persoonlijkheidsrechten ex. art. 25 Aw, en de geportretteerde op zijn zogenaamde portretrecht ex artt. 19-21 Aw. Deze worden verder buiten beschouwing gelaten.[160]

(3) Beperkingen op het auteursrecht

Niet iedere openbaarmaking of verveelvoudiging levert een inbreuk op het auteursrecht op. In de Auteurswet zijn enkele beperkingen opgenomen ten aanzien van het auteursrecht.[161] Zo is het toegestaan om voor eigen oefening, studie of gebruik werken te verveelvoudigen (art. 16b-c Aw, privékopie) en is het onder voorwaarden toegestaan om werken over te nemen (art. 15 Aw, persexceptie) en te citeren (art. 15a Aw).[162] Ook kan gedacht worden aan de parodie-exceptie (art. 18b Aw). Tot slot dient nog opgemerkt te worden dat erop sommige onderdelen van het hiervoor geschetste bijzondere regelingen bestaan zoals fotografische werken en filmwerken bijvoorbeeld ten aanzien van het citaatrecht. Omdat het hier aanvullende voorwaarden betreft en geen afwijking van de hiervoor gestelde hoofdregels blijven deze verder buiten beschouwing. Om te voorkomen dat iedere internetgebruiker altijd inbreuk zou maken op het auteursrecht geldt ook de incidentele technisch noodzakelijke kopie (art. 13 a

[157] Vgl. privékopie (art. 16 Aw); citaatrecht (art. 15a Aw) en de incidentele technisch noodzakelijke kopie (art. 13 a Aw).
[158] Art. 3 Richtlijn 2001/29 van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij' (Auteursrechtrichtlijn).
[159] Zie ook Visser 2010, p. 14.
[160] Zie voor een meer inhoudelijke behandeling van het persoonlijkheidsrecht en het portretrecht o.m. het standaardwerk van Spoor/Verkade/Visser 2005, p. 303; en in relate tot software Struik, Van Schelven & Hoorneman 2010, p. 135.
[161] Zie voor een meer inhoudelijke behandeling van de beperkingen o.m. het standaardwerk van Spoor/Verkade/Visser 2005, p. 211; en in relate tot software Struik, Van Schelven & Hoorneman 2010, p. 18.
[162] Eerder is al gewezen op HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie) heeft geconstateerd dat een reproductie uit een ongeoorloofde bron niet als een uitzondering voor privé-kopiëren kwalificeert.

Aw) als een beperking op het auteursrecht.[163] Dit betekent dat niet iedere kopie van bijvoorbeeld een foto direct een inbreuk op het auteursrecht oplevert. Zo kan een afbeelding van een boekomslag op een blog waarin een recensie geschreven wordt over het afgebeelde boek een beeldcitaat vormen dat zolang de regels van het citaatrecht gevolgd zijn geen inbreuk op het auteursrecht oplevert. Met name een beroep op de wettelijke beperkingen maakt het voorlopig lastig voor de rechthebbende om het proces van detectie van het watermerk tot het versturen van een sommatiebrief volledig te automatiseren. Tot het arrest van het HvJ inzake ACI Adam/Stichting De Thuiskopie was het in Nederland toegestaan om content te downloaden uit illegale bron.[164] Met kort gezegd een verbod op downloaden uit illegale bron is de relevantie van het watermerk als bewijsmiddel toegenomen. Het watermerk kan dan immers ook worden ingezet bij de opsporing wanneer een computer of andere drager in beslaggenomen is. Het watermerk kan in dit geval duidelijk maken of de gebruiker van de content beschikt over de juiste licentie of niet.

Ten slotte rest de vraag wanneer er sprake is van inbreuk op het werk van de rechthebbende door de kopie of het gelijkende object van de wederpartij. Daarvan is sprake wanneer een werk in 'zodanige mate de auteursrechtelijk beschermde trekken van het eerdere werk vertoont dat de totaalindrukken die de beide werken maken te weinig verschillen voor het oordeel dat het eerstbedoelde werk als een zelfstandig werk kan worden aangemerkt'.[165] Of zoals Visser het verkort weergeeft: 'Het lijkt te veel als het te weinig verschilt', terwijl er geen toestemming van de rechthebbende is.[166] Wanneer dat precies het geval is, is op voorhand niet altijd vast te stellen. Bij een letterlijke of identieke kopie, zoals bij het posten van een film- of muziekwerk op internet is de totaalindruk altijd gelijk en is er dus sprake van inbreuk op het auteursrecht. Het is uiteindelijk de rechter die beslist over de vraag of er sprake is van inbreuk of niet.[167] Verder kan nog worden opgemerkt dat er buiten het auteursrecht ook sprake kan zijn van onrechtmatig handelen.[168]

3.4.1.2 België

In België heeft alleen de auteur van een werk van letterkunde of kunst het recht het werk ongeacht welk procédé mede te delen aan het publiek, te reproduceren en zijn werk te distribueren (art. 1 Aw). Evenals in Nederland is er sprake van inbreuk op het auteursrecht wanneer (1) een werk (2) beschikbaar wordt gesteld voor het publiek en/of wordt

[163] De Nederlandse wetgever kwalificeert het strikt genomen niet als een beperking omdat zij het uitsluit van het verveelvoudigingsbegrip. De richtlijn kwalificeert het wel als een beperking.
[164] HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie).
[165] HR 29 november 2002, NJ 2003, 17, TBR 2003, p. 224 m.nt. Quanjel-Schreurs, AMI 2003, p. 15 m.nt. Visser (Accordo/Tros).
[166] Visser 2011b, p. 323.
[167] Dat rechter daar verschillend over kunnen denken laat Visser 2011a in diverse voorbeelden zien in inzake de Tripp Trapp stoel .
[168] Zie o.m. Vzr Rb. Arnhem, 22 mei 2008, ECLI:NL:RBARN:2008:BD3441 (De Roode Roos) waar de rechter bij gebrek aan een eigen oorspronkelijk karakter geen auteursrecht aan nam op gewatermerkte productiefoto's, maar hier de gedraging wel als onrechtmatig beoordeeld (ov. 4.11).

gedistribueerd zonder dat degene die de handelingen verricht hiervoor toestemming heeft verkregen van de rechthebbende (licentie) of (3) een beroep kan doen op de zogenoemde wettelijke beperkingen of uitzonderingen op de vermogensrechten van de auteur. De wettelijke omschrijving in België is hiermee meer in overeenstemming met de richtlijnen.[169]

(1) Werk van rechthebbende moet auteursrechtelijk beschermd zijn

Om inbreuk op het auteursrecht te kunnen vaststellen zal eerst vastgesteld moeten worden dat er sprake is van een auteursrechtelijke beschermd werk. Dat betekent dat het object van de eiser zelf voor bescherming in aanmerking moet komen. Het werkbegrip is in beginsel een nationaal begrip, maar wordt in Europees verband (art. 2 Rl. 2001/29/EG) inmiddels door het Hof van Justitie EU steeds vaker ingevuld.[170] In België geldt dat er sprake is van een werk wanneer het object oorspronkelijk is in die zin dat het gaat om een eigen intellectuele schepping (EIS) van de auteur. Hierbij is niet vereist dat het de stempel draagt van de persoonlijkheid van de maker.[171] Het Hof van Cassatie volgt hierbij het HvJ EU, met uitzondering van de persoonlijkheid van de maker.[172] Volgens het HvJ EU staat de keuze van de auteur centraal.[173] Wanneer de oorspronkelijkheidsdrempel wordt bereikt geldt dat de beschermingsomvang van alle werken gelijk is.[174] Het werkbegrip is en wordt onder leiding van het HvJ EU steeds verder geharmoniseerd waardoor van verschillen tussen Nederland en België ten aanzien van het werkbegrip in de toekomst nauwelijks meer sprake zal zijn. Voor de in dit onderzoek bedoelde werken (muziek, films en foto's) zal in de regel sprake zijn van auteursrechtelijk beschermde werken. Evenals Visser in Nederland, concludeert ook Deene in België dat het zowel voor een auteursrechthebbende als voor een inbreukpleger koffiedik kijken is of een creatie door een rechtscollege al dan niet als origineel zal wordt beschouwd.[175]

(2) Distributie en beschikbaarstelling voor het publiek

Ook de kernbevoegdheden zijn in België voorbehouden aan de auteur waardoor hij als enige bevoegd is om zijn werk mede te delen aan het publiek, te reproduceren en te distribueren, behoudens de beperkingen bij wet gesteld. Zonder diens voorafgaande toestemming is er ook

[169] Zie par. 3.4. Dat is overigens niet op alle punten het geval. Zie Deene & Van der Perre 2005.
[170] Zie voetnoot 127.
[171] Cass. 26 januari 2012, C.11.0108.N, IEFBE 150, IRDI, 2012/2 m.nt F. Gotzen. Hiermee is het Hof van Cassatie teruggekomen op eerdere beslissingen waarin de persoonlijkheid van de maker nog wel een rol speelde/ Zie o.m. Cass. 11 maart 2005 AM 2005, 396, m.nt. F. De Visscher; Cass. 27 april 1989, RW 1989-90, 362. Vgl. hier ook de Europese rechtspraak waarin het HvJ EU wel uitdrukking geeft aan de persoonlijkheid van de auteur. Zie o.m. HvJ EU, 16 julo 2009, C-5/08 (infopaq), ov. 32-39, AMI 2009, p. 473-488 m.nt. B. Michaux; HvJ EU 1 december 2011, zaak C-145/10 (Eva Maria Painer), ov. 97 en 155.
[172] HvJ EU 16 juli 2009, Infopaq International, C-5/08, Jur. p. I-6569, punt 37; laatste herhaald in HvJ EU 4 oktober 2011, C-403/08 en C-429/08, IEF 10286, ov. 97 (Premier League).
[173] HvJ EU 1 december 2011, zaak C-145/10 (Eva Maria Painer), ov. 87-92.
[174] HvJ EU 1 december 2011, zaak C-145/10 (Eva Maria Painer), ov. 97-99.
[175] Waar de willekeur in Nederland duidelijk wordt aan de hand van de TRIPP-TRAPP-stoel, maakte Deene (2010, p. 443) dat duidelijk aan de hand van een zaak over wandtapijten met uitzichten van historische steden.

in België sprake van inbreuk op het auteursrecht. Voor het uploaden van werken is met name van belang dat de gedaagde het desbetreffende werk heeft meegedeeld aan het publiek of geproduceerd. Deze 'nationale' begrippen (art. 1 Aw) zijn inmiddels geharmoniseerd in de auteursrechtrichtlijn (Art. 3 en 4 Rl. 2001/29/EG) en moeten volgens het HvJ EU in de gehele EU autonoom en eenvormig worden uitgelegd.[176] Ook in België wordt uploaden als een publieke mededeling en reproductieproces gezien waarvoor toestemming noodzakelijk is.[177]

(3) Beperkingen op het auteursrecht

Niet iedere mededeling aan het publiek of reproductie levert een inbreuk op het auteursrecht op. Ook in de Belgische auteursrechtwet zijn beperkingen opgenomen ten aanzien van het auteursrecht. Zo is het onder voorwaarden toegestaan om werken over te nemen en te citeren (art. 21-22 Aw.). Om te voorkomen dat iedere internetgebruiker altijd inbreuk zou maken op het auteursrecht geldt ook de incidentele technisch noodzakelijke kopie (Artikel 21 §3 Aw/) als een beperking op het auteursrecht.[178] In België was het tot het arrest van het HvJ inzake ACI Adam/Stichting De Thuiskopie onduidelijk of downloaden in België onder de beperkingen van met name de thuiskopie zou vallen of niet.[179] De relevantie van het watermerk als bewijsmiddel is door deze uitspraak van het Hof ook hier toegenomen. Een betrouwbaar watermerk kan nu immers zowel als bewijs dienen in het geval content wordt geupload als in gevallen wanneer content wordt gedownload.[180]

Ten slotte rest de vraag wanneer er sprake is van relevante gelijkenis tussen het werk van de rechthebbende en de kopie of het gelijkende object van de wederpartij. Evenals in Nederland speelt ook daar de totaalindruk een belangrijke rol.[181] Het Hof van Cassatie geeft aan de feitenrechter mee dat bij opvallende gelijkenissen met eerder bestaand werk beoordeeld moet worden of deze gelijkenissen toevallig zijn, dan wel voorkomen uit bewuste of onbewuste ontlening aan dat werk.[182] Volgens het Hof van beroep in Antwerpen moet evenals in Nederland bij de beoordeling van een inbreuk op het reproductierecht eerder rekening gehouden worden met de punten van gelijkenis dan met de punten van verschil bij een globale

[176] HvJ EU 7 december 2006 zaak 306/05 (Rafael Hoteles), ov. 31.
[177] Art. 1 § 1 lid 3 Aw. Zie verder o.m. Werkers e.a. 2009, p. 18-19 en de daar aangehaalde literatuur.
[178] Een verschil met het Nederlandse recht ligt hier in de bewijslast. In Nederland is het voor inbreuk aan de rechthebbenden zijn om te bewijzen dat een reproductie niet onder de voorwaarden van de tijdelijke technische reproductie valt. In België moet de gebruiker dit bewijs leveren dat hij wel een beroep kan doen op art. 21 § 3 Aw. Zie Deene & Van der Perre 2005, p. 870.
[179] In HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie) maakt het Hof duidelijk dat downloaden uit illegale bron niet is toegestaan. Voor het arrest waren wetten in voorbereiding die illegaal downloaden zouden verbieden. Zie o.m. wetsvoorstel (DOC 53 1120/001), strekkende tot een betere bescherming van culturele creaties op het Internet (ingediend door de heer David Clarinval c.s.)
[180] Het watermerk kan dan immers ook worden ingezet bij de opsporing wanneer een computer of andere drager in beslaggenomen is. Het watermerk kan in dit geval duidelijk maken of de gebruiker van de content beschikt over de juiste licentie of niet. In dit geval kan het watermerk dus ook als bewijs dienen voor de gebruiker van de content om aan te tonen dat hij wel degelijk over de juiste licentie beschikt. Zie ook 3.4.1.1 onder (3) Beperkingen op het auteursrecht.
[181] Cass. 25 september 2003, RW 2003-2004, 1179;
[182] Cass. 3 september 2009, IRDI 2009, 411, m.nt. M. Buydens (C.08.0337.N)

indruk.[183] Voor zover relevant voor dit onderzoek kan worden gesteld dat bij een letterlijk of identieke kopie de totaalindrukken gelijk zijn en er dus sprake is van inbreuk. Het is uiteindelijk ook hier de rechter die beslist over de vraag of er sprake is van inbreuk of niet.

3.4.1.3 Tussenconclusie

Om te kunnen bepalen welke rol het watermerk kan spelen bij het vaststellen van inbreuk op het auteursrecht is in deze paragraaf kort ingegaan op de vraag wanneer er sprake is van inbreuk op het auteursrecht naar civiel recht.

Het inbreukcriterium wordt in de verschillende EU jurisdicties verregaand geharmoniseerd ingevuld en uitgelegd. Hierdoor zijn ervoor het vaststellen van inbreuk op het auteursrecht weinig relevante verschillen waarneembaar tussen Nederland en België. Deze overeenstemming kan voornamelijk worden verklaard vanuit het streven van het HvJ EU om met betrekking tot de begrippen uit de richtlijn steeds meer te komen tot een eenvormige communautaire interpretatie. In hoeverre dat in de toekomst verdere vormen aanneemt blijft afwachten omdat ook het Hof van Cassatie recentelijk een arrest wees ten aanzien van het werkbegrip en daarbij afweek van de door het HvJ EU gebezigde eenvormige communautaire interpretatie.

Om te kunnen bepalen welke rol het watermerk kan spelen bij het vaststellen van inbreuk op het auteursrecht is in de voorgaande paragraaf kort ingegaan op de vraag wanneer er sprake is van inbreuk op het auteursrecht naar het civiele recht. De voorgaande beschouwing laat zien dat er overeenkomstig Europese richtlijnen in beide landen geldt dat het uitsluitend recht om een werk te reproduceren, ter beschikking te stellen en mededeling daarvan te doen aan het publiek, is voorbehouden aan de maker van een werk van letterkunde of kunst. Omdat de rechthebbende in de regel in een licentie-overeenkomst het recht voorbehoud het werk kort gezegd op internet te plaatsen, pleegt de licentienemer inbreuk wanneer hij dit wel doet. Het watermerk kan dan als bewijsmiddel dienen om een verband te leggen tussen de licentienemer en de inbreuk op het auteursrecht. Het watermerk is in geen geval voldoende om inbreuk op het auteursrecht als zodanig te bewijzen. Daarvoor zijn meer vaststellingen nodig.

Doordat het aan de wederpartij is om een beroep te doen op een wettelijke beperking is er behoudens een ‘handmatige’ vaststelling dat er sprake is van inbreuk op het werk in beginsel geen beletsel om het proces volledig te automatiseren door een softwareprogramma. Na detectie en interpretatie van het watermerk kunnen de gegevens van de licentienemer dan gekoppeld worden aan een standaardsommatiebrief. Het lijkt mij, evenals de praktijk bij Getty Images heeft laten zien, echter geen wenselijke scenario vanwege het gebrek aan zorgvuldigheid.[184]

[183] Hof van Beroep Antwerpen 15 juni, 2009, 2008/AR/1087, NJW 2010/225, p. 447.
[184] Getty images lijken het proces, gezien de brieven die zij versturen helemaal geautomatiseerd te hebben. Zie voor de praktijken Getty Images en kritiek daarop o.m. Sandvliet & Engelfriet 2012, p. 204; en op IE-forum.nl,

In de uitspraak van het HvJ EU inzake ACI Adam/Stichting De Thuiskopie heeft het Hof kort gezegd duidelijk gemaakt dat downloaden uit illegale bron niet is toegestaan. Hiermee is duidelijk geworden dat zowel het uploaden als downloaden van content zonder toestemming van de rechthebbende niet is toegestaan. Daarmee is de relevantie van het watermerk als bewijsmiddel toegenomen.[185] Het watermerk kan nu ook worden ingezet bij de opsporing van onrechtmatig verkregen downloads, bijvoorbeeld bij de opsporing van in beslaggenomen computers of andere dragers van content. In dit voorbeeld kan het watermerk duidelijk maken of iemand over een licentie beschikt of niet. Om verdere zoekkosten te voorkomen is het raadzaam om in het watermerk op te nemen of de licentienemer beschikt over een licentie die bijvoorbeeld verdere distributie op het internet toestaat. In dat geval zal in veel gevallen direct duidelijk zijn of er sprake is van een schending van de licentie-overeenkomst of niet.

3.4.2 Inbreuk op het auteursrecht als strafbaar feit

In de navolgende paragrafen wordt onderzocht wanneer er mogelijk sprake is van inbreuk op het auteursrecht naar Nederlands en naar Belgisch strafrecht.

3.4.2.1 Nederland

Naast de civielrechtelijke handhaving is het ook mogelijk dat de inbreukmaker strafrechtelijk wordt vervolgd. In een strafrechtelijke procedure is de tenlastelegging voor de rechter leidend en gaat het om de vraag of de verdachte het tenlastegelegde feit heeft begaan.[186] Het OM snijdt in de praktijk de tenlastelegging toe op een wettelijke delictsomschrijving die hij van toepassing acht.[187] Daartoe zal in dit onderzoek de wettelijke delictsomschrijving van artikel 31 en 31a Aw als uitgangspunt worden genomen.[188] Het is vervolgens aan het OM om te bewijzen dat de in de tenlastelegging neergelegde feiten hebben plaatsgevonden.

In de artikelen 31 en 31a Aw zijn respectievelijk de opzettelijke inbreuk en opzettelijke verspreiding opgenomen.

IEF 10295; IEF 10265. Inmiddels (2014) lijkt Getty Images haar beleid te hebben aangepast http://ipkitten.blogspot.nl/2014/03/getty-images-goes-free-is-embedding.html.

[185] HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie).

[186] Zie daarvoor verder hoofdstuk 4.

[187] Hij is hiertoe ook verplicht op grond van art. 6 lid 3, sub a EVRM. Vgl. art. 261 lid 1 Sv. Zie o.m. Corstens 2008, p. 727 en Nijboer 2011, p. 30.

[188] In de praktijk worden de meeste zaken rondom op onrechtmatige wijze het beschikbaar stellen van video, muziek en foto's gebaseerd op de artikelen 31 en 31a Aw, vaak in combinatie met artikel 31b Aw waarin de beroepsmatige variant is opgenomen. Zie o.m. Hof 's-Hertogenbosch 27 september 2004, ECLI:NL:GHSHE:2004:BQ1759; Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268; Hof Arnhem 3 maart 2009, ECLI:NL:GHARN:2009:BI1243; Rb. Leeuwarden 9 april 2009, ECLI:NL:RBLEE:2009:BI0666; Rb. Amsterdam 26 november 2009, ECLI:NL:RBAMS:2009:BK7336; Hof 's-Gravenhage 22 oktober 2010, ECLI:NL:GHLEE:2010:BM3169; Hof Leeuwarden 4 mei 2010, ECLI:NL:GHSGR:2010:BO8246; Hof's-Hertogenbosch 30 maart 2011, ECLI:NL:GHSHE:2011:BP9521.

Artikel 31 Aw (opzettelijke inbreuk)
'Hij, die opzettelijk inbreuk maakt op eens anders auteursrecht, wordt gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie.'

Artikel 31a (opzettelijke verspreiding)
Hij die opzettelijk een voorwerp waarin met inbreuk op eens anders auteursrecht een werk is vervat,
a. openlijk ter verspreiding aanbiedt,
b. ter verveelvoudiging of ter verspreiding voorhanden heeft,
c. invoert, doorvoert, uitvoert of
d. bewaart uit winstbejag
wordt gestraft met gevangenisstraf van ten hoogste één jaar of geldboete van de vijfde categorie.

Voor het begrip auteursrecht wordt aansluiting gezocht bij de artikelen, 1, 12, 13 en 14 Aw. In beginsel wordt erop basis van de bijbehorende civielrechtelijke jurisprudentie invulling gegeven aan de vraag of er sprake is van een inbreukmakende handeling. Ook in het strafrecht is het de verdachte zelf die toepasselijke auteursrechtelijke beperkingen moet aanvoeren, bijvoorbeeld om duidelijk te maken dat er sprake is van een privékopie en hij derhalve een toegestane inbreuk maakt op het auteursrecht.[189]

De inhoud van het auteursrecht wordt gevormd door de aan de maker voorbehouden rechten om het werk openbaar te maken (art. 12 Aw) en te verveelvoudigen (art. 13 en 14 Aw). Aan deze begrippen wordt ook in het strafrecht een ruime betekenis toegekend.[190] Het uploaden van bestanden die auteursrechtelijk beschermde werken bevatten en waarvoor de toestemming van de rechthebbende ontbreekt levert inbreuk op het auteursrecht op. Indien dit uploaden zonder toestemming opzettelijk plaatsvindt, is in beginsel sprake van het strafbare feit van artikel 31 Auteurswet.[191] Bij verveelvoudigingen (art. 13) wordt de opdrachtgever met de vervaardiger in eigen persoon gelijk gesteld.[192] Ook het laten kopiëren van studieboeken is daarmee onder meer strafbaar.[193] Het OM zal in de dagvaarding moeten stellen dat het gaat om een auteursrechtelijk beschermd werk, dat er inbreuk is gemaakt en op welke wijze de verdachte dat werk openbaar heeft gemaakt of verveelvoudigd.[194]

Voor de delictsomschrijving van artikel 31a en artikel 31 dient verder aansluiting te worden gezocht bij de wettelijke formulering van inbreuk en opzet. Het is voor het opzetbegrip in artikelen 31 en 31a Aw voldoende om voorwaardelijke opzet (kansopzet) te bewijzen.[195] De

[189] Verkade, T&C 2013, aant. 2.
[190] Zie par. 3.4 en voor een ruimte uitleg van het begrip openbaar maken in het strafrecht o.m. HR 16 december 1986, NJ 1987, 613 (Verhuur illegale kopieën), alsmede de conclusie van A-G Leijten voor historisch overzicht.
[191] Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey).
[192] TK 7877, 1964 - 1965, nr. 3, MvT, p. en TK 7877, 1968-1969, nr. 6, MvA, p. 6.
[193] HR 13 december 1988, ECLI:NL:HR:1988:AC3339 (Verveelvoudiging van studieboeken)
[194] Zie Gerbrandy 1973, Kort commentaar op de auteurswet 1912, p. 248; Hof Amsterdam 14 mei 1929, NJ 1930 1616; Bijvoorbeeld: verdachte, op een of meer tijdstip(pen) gelegen in of omstreeks de periode van 18 april 2003 tot en met 14 december 2004 (telkens) te Rotterdam en/of Maarssen en/of (elders) in Nederland, (telkens) tezamen en in vereniging met een andere of anderen, althans alleen (telkens) opzettelijk inbreuk heeft gemaakt op het auteursrecht van (een) ander(en), te weten: Warner, en/of een of meer andere rechthebbende(n).
[195] HR 9 november 1954, NJ 1955, 55, m.nt. WP. (Cicero).

voorwaardelijke opzet ziet hier zowel op het inbreukmakende karakter als op de onder a t/m d geformuleerde handelingen en in dit onderzoek met name het onder a genoemde geval.
Het standaardarrest voor voorwaardelijke opzet betreft een auteursrechtkwestie. Op verzoek van het bestuur van toneelvereniging 'Cicero' heeft het Internationale Bureau voor Auteurs- en Opvoeringsrechten (hierna: IBVA) 'Holland' bekend gemaakt dat voor het opvoeren van het stuk 'De man in burger' een vergoeding verschuldigd was van fl. 25,- en de afname van acht tekstboekjes.[196] De toneelvereniging voldeed aan de eerste voorwaarde door de vergoeding te betalen, maar weigerde om de acht tekstboekjes af te nemen. In haar verweer gaf de toneelvereniging hiervoor als reden dat deze voorwaarde 'zonder recht gesteld werd' en 'zo zij al bekend waren met het feit dat deze voorwaarde veelal gesteld placht te worden, zij ook wisten dat dat zeer herhaaldelijk ten onrechte geschiedde'. Om na te gaan of deze voorwaarde inderdaad ten onrechte was gesteld vraagt de toneelvereniging aan het IBVA namens wie zij deze voorwaarde stelt. Uit de omstandigheid dat zelfs het IBVA niet op de hoogte bleek, namens wie zij de voorwaarde stelde maakt de toneelvereniging op dat niet is na te gaan of de voorwaarde ten onrechte is gesteld of niet. De toneelvereniging stelt zich dan op het standpunt dat wanneer bij het stellen van deze voorwaarde niet blijkt, dat dit namens degene geschiedt, die daartoe gerechtigd is er geen sprake kan zijn van inbreuk op het auteursrecht. De Hoge Raad gaat niet in die gedachte mee en stelt dat hij die 'zich ervan bewust [is] dat de vertegenwoordiger van den rechthebbende hem tot de opvoering slechts vergunning geeft indien hij aan twee daartoe gestelde eisen voldoet, daarop den enen eis vervullende den anderen bepaaldelijk niet vervult, zonder te weten of deze ten onrechte werd gesteld, en dan desalniettemin, in stede van vooraf daarnaar te informeren, tot de opvoering overgaat, zich willens en wetens blootstelt aan de geenszins als denkbeeldig te verwaarlozen kans, dat die vertegenwoordiger ook dergelijken tweeden eis niet zonder grond zal hebben gesteld. Door niet verder te informeren hebben de bestuurders de niet te verwaarlozen kans laten bestaan dat men inbreuk zou plegen op het auteursrecht. Dat betekent dat de verdachte zich 'zich willens en wetens blootstelt aan de geenszins als denkbeeldig te verwaarlozen kans' dat er inbreuk wordt gemaakt'.[197]

Voor overtreding van artikel 31 Aw zal moeten worden vastgesteld dat de inbreukmaker opzettelijk inbreukmakende handelingen heeft verricht. Om tot een bewezenverklaring te kunnen komen zal het OM moeten bewijzen dat er sprake is van (voorwaardelijke) opzet op het verrichten van deze openbaarmakings- dan wel verveelvuldigingshandelingen. De vraag

[196] In deze zaak is het driekoppige bestuur als verdachte aangemerkt. De toneelvereniging bezat geen rechtspersoonlijkheid. Gerbrandy 1973, p. 248 merkt onder verwijzing naar verschillende uitspraken op dat er destijds nogal wat variatie was in de wijze waarop het OM de hoofdverdachten uitzocht.
[197] Waar de Hoge Raad ten tijde van het Cicero-arrest nog sprake van het 'zich willens en wetens blootstellen aan de geenszins als denkbeeldig te verwaarlozen kans' geldt thans dat voor voorwaardelijk opzet een 'aanmerkelijke' kans is vereist. Zie o.m. HR 19 februari 1985, NJ 1985, 633 (Cocaïne in koffer); HR 20 februari 2007, NJ 2007, 313 m.nt. Buruma (HIV-III) en de vaak afwijkende mening van de verschillende AG's in de desbetreffende HIV-arresten.

of en wanneer er sprake is van voorwaardelijk opzet laat ik verder buiten beschouwing omdat het watermerk daar in geen geval een bewijsrechtelijke bijdrage aan kan leveren.[198]

Aangetoond moet worden dat de verdachte de werken heeft geopenbaard (geupload) en/of verveelvoudigd, zonder toestemming van de rechthebbende. Het gebrek aan toestemming zal beginnen met de stelling dat er geen toestemming is gegeven. Vervolgens is het aan de verdachte om duidelijk te maken dat er wel sprake is van toestemming of in ieder geval op omstandigheden wijzen die erop duiden dat er wel toestemming is verkregen. De opzet ontbreekt als er redelijkerwijs vanuit mag worden gegaan dat er wel betaald is en daarmee toestemming is verkregen.[199] Uit de gepubliceerde rechtspraak blijkt dat het rechthebbenden vaak wel lukt om aannemelijk te maken dat er sprake is van het uploaden van auteursrechtelijke beschermd materiaal, maar dat van zelfstandig bewijs zelden sprake is.[200]

3.4.2.2 België

In België is het inbreuk plegen op het auteursrecht strafbaar gesteld in de vorm van het misdrijf van namaking.[201] Voor de rechter is de tenlastelegging van het OM daarvoor leidend.[202] In het kader van het watermerk is het van belang om te bepalen of het relevant is voor de in de tenlastelegging te bewijzen feiten. Het OM snijdt in de praktijk de tenlastelegging toe op een wettelijke delictsomschrijving die hij van toepassing acht.[203] Daarbij zal in dit onderzoek de wettelijke delictsomschrijving van artikel 80 Aw als uitgangspunt worden genomen. Het is vervolgens aan het OM om te bewijzen dat de in de tenlastelegging neergelegde feiten hebben plaatsgevonden.

Inbreuk op het auteursrecht wordt in artikel 80 Aw strafbaar gesteld als misdrijf en onderscheidt drie verschillende misdrijven van namaking (mijn nummering SLG):

> (1) Hij die kwaadwillig of bedrieglijk inbreuk pleegt op het auteursrecht en de naburige rechten, is schuldig aan het misdrijf van namaking.
> (2) Hetzelfde geldt voor de kwaadwillige of bedrieglijke aanwending van de naam van een auteur of van een persoon die een naburig recht geniet, of voor enig door hem gebruik distinctief kenmerk

[198] Hiervoor verwijs ik naar de handboeken strafrecht (Corstens 2014, Noyen/ T&C). Voor het invullen van de opzet is het voldoende om de voorwaardelijke opzet aan te tonen. Hoewel het watermerk weinig zegt over opzet ten tijde van het delict, lijkt voorwaardelijke opzet mij strafrechtelijk gezien niet moeilijk te bewijzen, nu slechts relevant is of er een aanmerkelijke kans was dat de licentienemer zonder toestemming van de rechthebbende voor het openbaar maken en verveelvoudigen van de content inbreuk maakt op het auteursrecht. In het licht van het Cicero-arrest kan de verdachte zich immers niet verschuilen achter de stellingname dat hij het niet wist.
[199] Rb. 'Hertogenbosch 24 maart 1941, NJ 1941, 783; Gerbrandy 1973, p. 248.
[200] Zie o.m. Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey), (feit 1). In deze zaak maakte het zgn. Brein-dossier met postings door onder andere verdachte downloads en uploads weliswaar aannemelijk dat de werking van de website gericht is op het uploaden van bestanden, maar vormen geen zelfstandig bewijs dat de verdachte zelf werken geupload.
[201] Artikel 79bis t/m 86 Auteurswet.
[202] Zie daarover o.m. Verstraeten 2012, p. 967; Hof van Beroep Gent, 6 oktober 2004 (Me to you).
[203] Hij is hiertoe ook verplicht op grond van art. 6 lid 3, sub a EVRM.

> om zijn werk of prestatie aan te duiden. De aldus tot stand gebrachte voorwerpen worden als nagemaakt beschouwd.
> (3) Hij die voorwerpen, wetende dat zij nagemaakt zijn, verkoopt, verhuurt, te koop of te huur stelt, in voorraad heeft voor de verkoop of de verhuur of in België invoert voor commerciële doeleinden, is schuldig aan hetzelfde misdrijf. (…).

In de artikelen 79bis, § 1, 79ter Aw zijn eveneens omzeiling van technische voorzieningen en verwijdering of wijziging van elektronische beheersinformatie alsmede de verspreiding daarvan als misdrijf strafbaar gesteld (vgl. art. 6 en 7 ARl). Voor al deze misdrijven geldt dat een gevangenisstraf kan worden opgelegd van drie maanden tot drie jaar en een geldboete van 100 tot 100.000 euro. In de praktijk wordt de boete vermenigvuldigd met de factor 5,5 vanwege de opdecimes op de strafrechtelijke boete waardoor de werkelijk te betalen geldboete gelijk is aan 550 tot 550.000 euro.[204] Hoewel het geen straf is, wordt de veroordeelde volgens Maeyaert vaak verplicht om een bedrag van 10 euro te betalen als bijdrage aan het Fonds tot hulp aan slachtoffers van opzettelijke geweldsdaden.[205] Daarnaast dient hij in te staan voor de vergoeding van gerechtskosten in strafzaken.[206] Deze vergoeding is evenmin een straf.[207] De bepalingen van boek I van het Strafwetboek, met inbegrip van hoofdstuk VII (strafbare deelneming) en artikel 85 (verzachtende omstandigheden), zijn in artikel 80 Aw tevens van toepassing verklaard op het misdrijf van namaking.[208] Hierdoor is ook de poging tot dit misdrijf strafbaar gesteld. Vanuit het commune strafrecht bezien wordt het hierdoor ook mogelijk om strafbepalingen van organiseerde misdaad toe te passen.

Het materiële element van deze strafrechtelijke aansprakelijkheid, dat wil zeggen de inbreuk op het auteursrecht, waaronder zowel het vermogensrecht als de morele rechten, zal door de strafrechter moeten worden beoordeeld op grond van de Auteurswet en is hiermee gelijk gesteld aan het civiele recht.[209] Dat geldt overigens ook voor de vordering tot schadeloosstelling.[210] Hierbij moet wel worden opgemerkt dat het auteursrecht in een burgerlijk geding wordt beoordeeld door gespecialiseerde rechters in vijf gecentraliseerde rechtbanken tegen de zeventwintig correctionele rechtbanken.[211] Het uploaden van bestanden

[204] Opdecimes zijn de voorgeschreven verhoging van strafrechtelijke geldboeten vanwege muntontwaarding. Wet van 5 maart 1952, BS 3 april 1952; Wet van 26 juni 2000 betreffende de invoering van de euro, BS 29 juli 2000; Wet van 7 februari 2003 houdende diverse bepalingen inzake verkeersveiligheid, BS 25 februari 2003.
[205] Cass. 30 juni 1993, Pas. 1993, 635. Dit vindt plaats op grond van artikel 28 en 29 Wet 1 augustus 1985 houdende fiscale en andere bepalingen, BS 6 augustus 1985, inwerking getreden op 18 december 1986. Ook dit bedrag wordt vermeerderd met opdecimes.
[206] Artikel 71 wet 28 juli 1992, Koninklijk Besluit van 11 december 2001, BS 22 december 2001.
[207] Cass. 9 november 1994, JT 1995, 214.
[208] Zie o.m. Hof van Beroep Antwerpen, 23 mei 2003 onder verwijzing naar Cass. 13 september 1994, A.C. 1994, 733 (niet gepubliceerd, opgenomen in Maeyaert 2012, p. 451).
[209] Maeyaerts 2012, p. 438.
[210] Zie o.m. Van Damme 2009, p. 282.
[211] Dat de centralisatie alleen geldt voor civiele zaken en niet voor het strafrecht wordt in de literatuur betreurd omdat het risico van verschillende beoordelingen hierdoor toeneemt. (zie o.m. Van Damme 2009, p. 273). Burgerlijke gedingen zowel in eerste aanleg (rechtbank) als in hoger beroep (Hof van Beroep) spelen in Gent, Antwerpen, Brussel, Bergen en Luik. Dit geldt ook voor zaken in kort geding en procedures op eenzijdig verzoekschrift. Dit geldt niet voor de territoriale bevoegdheid van vredesrechters voor auteursrechtgeschillen met een geringe waarde.

zonder toestemming van de auteursrechthebbende is ook strafrechtelijk niet toegestaan. Het morele element van de aansprakelijkheid ziet op bijzondere opzet van kwaadwillig of bedrieglijkheid waarmee de inbreuk moet zijn gepleegd.[212] In de parlementaire voorbereiding van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten (hierna: WNP) is kwaadwillig omschreven als 'de wil om de al dan niet materiële belangen van de rechthebbende te schaden'.[213] Daarvan is in de jurisprudentie sprake wanneer de namaking erop gericht is om de auteur moreel te krenken, hetzij in zijn eer, hetzij in zijn inkomsten.[214]

In tegenstelling tot andere IE-rechten is het voor de toepassing van de strafrechtelijke bepalingen bij inbreuk op het auteursrecht niet vereist dat de inbreuk plaatsvindt in het economische verkeer.[215] Hierdoor zijn ook inbreuken in de privésfeer strafrechtelijk vervolgbaar. Dat geldt vanzelfsprekend alleen in die gevallen die buiten de wettelijke uitzonderingen of beperkingen vallen, zoals de thuiskopie. Voor een veroordeling voor het misdrijf van namaking zal in een strafrechtelijke procedure kwaadwilligheid of bedrieglijkheid (bijzonder opzet) ten aanzien van de inbreuk moeten worden bewezen.[216] Bedrieglijk opzet wordt in WNP evenals in de literatuur omschreven als de wil om zichzelf of iemand anders een onrechtmatig, zelfs niet-financieel en onrechtstreeks voordeel te bezorgen.[217] In de rechtspraak wordt dit (zeer) ruim opgevat.[218] Voor de beoordeling van het voordeel of winstoogmerk is het verder niet relevant of er daadwerkelijk winst wordt gemaakt.[219] Ook wanneer er verlies wordt geleden kan er sprake zijn van een winstoogmerk. Het Hof van Beroep acht het voldoende wanneer er wordt vastgesteld dat de dader niet tot doel had een intellectueel eigendomsrecht aan te tasten, ook niet als de dader de winst niet noodzakelijk voor zichzelf wilde innen.[220] Werkers e.a. merken op dat in een commerciële context bijna iedere inbreuk op het auteursrecht die willens en wetens wordt gepleegd als bedrieglijk wordt gekwalificeerd.[221] Voor zowel inbreuk op het auteursrecht als voor deze laatste categorie geldt tevens dat 'herhaling binnen vijf jaar na een in kracht van gewijsde gegane veroordeling

[212] Er is hier een bijzondere opzet vereist. De algemeen opzet die naar Belgisch recht, vereist dat de dader willens en wetens een strafbare handeling verricht, voldoet dus niet.
[213] Parl. Stukken 2006-2007, DOC 51 2852/1 (MvT), p. 36.
[214] Zie o.m. Brussel 11 april 1969, RW 1968-69, 1622, RIDA 1969, 76 m.nt. J. Corbet. Zie ook Maeyaert 2012, p. 340; Brussel 19 februari 1997, Ing.Cons. 1997, 107; Gent 7 mei 2008, TSR 2008, 456; Hof van Beroep Brussel 19 maart 2013, 2012 CO 674, IEFBE 380 (EBVBA/X)
[215] Zie o.m. Cor. Rb. Kortrijk, 29 februari 2012, nr. 12/383, IEF 11029; IEFBE173 (OM gevoegd: VZW IFPI en SABAM tegen MINJAUW).
[216] Kwaadwillig ziet op het doel van het veroorzaken van schade, terwijl bedrieglijk betekent dat men voordeel wil halen uit de inbreuk of benadeling van andermans rechten.
[217] Parl. Stukken 2006-2007, DOC 51 2852/1(MvT), p. 36; Maeyaert 2008, p. 440; Van Damme 2009, p. 275.
[218] Maeyaert 2008, p. 440; Van Damme 2009, p. 275. Zie o.m. Hof van Beroep Luik, 7 mei 2003, AM 2005, 128; Hof van Beroep Antwerpen 11 oktober 2000, AM 2000, 357 (pornografische versie Jerommeke).
[219] Zie o.m. Corr. Rb. Verviers 8 november 1989, JLMB 1990, 717; Corr. Rb. Antwerpen 28 februari 2002, AM 2002, 340 inzake illegale software. Corr. Hasselt 3 mei 2002, IRDI 2002, 171.
[220] Hof van Beroep Luik 7 mei 2003, AM 2005, 128.
[221] Werkers e.a. 2009, p. 29. Bij een handeling ter goeder trouw ontbreekt de wil om te plegen waardoor bij het gebrek aan dat element ook de strafrechtelijk bepaling in beginsel geen toepassing heeft.

wegens dezelfde inbreuk' kan leiden tot een veroordeling tot het dubbele van de maximumstraf.[222]

In de Belgische auteurswet is een aantal aanvullende maatregelen opgenomen, zoals aanplakking van de veroordeling zowel binnen als buiten gebouwen van de veroordeelde (art. 78bis § 7 Aw); sluiting van de inrichting van de veroordeelde in het geval van herhaling (art.); toewijzing van ontvangsten en de verbeurdverklaarde voorwerpen aan de burgerlijke partij die daarmee in mindering kan worden gebracht op de schadevergoeding (art. 86 Aw). De toepassing van Boek I Strafwetboek maakt het mogelijk om ook de bijzondere verbeurd verklaring toe te passen, waardoor het mogelijk is om voorwerpen die eigendom zijn van de veroordeelde en gediend of bestemd waren voor het plegen van het misdrijf (art. 42, 1º Sw); zaken (art. 42, 2º Sw) en vermogensvoordelen die (rechtstreeks) uit het misdrijf voortkomen (art. 42, 3º Sw) verbeurd te verklaren.[223] Deze bijkomende straf kan echter pas worden uitgesproken na een veroordeling tot een hoofdstraf.[224] Daarmee zou de rechthebbende ook inzicht kunnen verkrijgen in de wijze waarop hij tot de inbreuk gekomen is. Voor rechtspersonen geldt steeds dat zij op grond van de Auteurswet steeds burgerlijk aansprakelijk zijn voor de veroordeling tot het betalen van vergoedingen van welke aard ook, die wegens overtreding van de wet die worden uitgesproken tegen hun bestuurders, vertegenwoordigers of aangestelden (art. 84 Aw). Ondanks de kritiek op de harmonisatie die de WNP moest bewerkstelligen zijn wel de bepalingen inzake opsporing en vaststellingen van strafrechtelijke inbreuken ook voor het auteursrecht toepasselijk gemaakt en zijn de straffen verhoogd.

3.4.2.3 Tussenconclusie

Om te kunnen bepalen welke rol het watermerk kan spelen bij het vaststellen van inbreuk op het auteursrecht is in deze paragraaf kort ingegaan op de vraag wanneer er sprake is van inbreuk op het auteursrecht naar civielrecht en strafrecht (par. 3.3.2).

In beide landen bestaan er strafrechtelijke sancties voor het opzettelijk uploaden van auteursrechtelijk beschermde werken. Voor de invulling van het begrip auteursrecht wordt in beide landen aangesloten bij het civiele recht. Naast de civielrechtelijke elementen zal in het strafrecht ook het element 'opzet' bewezen moeten worden. Wanneer bewezen kan worden dat de verdachte het bestand heeft geupload is er in de regel weinig bewijs meer nodig om de hier bedoelde opzet te bewijzen. Het watermerk kan in ieder geval geen bijdrage leveren aan het bewijs van opzet. De bijdrage van het watermerk blijft dan beperkt tot hetgeen reeds is

[222] Artikel 78bis § 7 Aw geeft de rechter ook de mogelijkheid 'aanplakking van het vonnis of van de door haar opgestelde samenvatting ervan bevelen gedurende de door haar bepaalde termijn zowel buiten als binnen de inrichting van de overtreder, evenals de bekendmaking van het vonnis of van de samenvatting ervan door middel van dagbladen of op enige andere wijze, en dit alles op kosten van de overtreder; zij kan bovendien de verbeurd verklaring bevelen van onrechtmatige winsten die met behulp van de inbreuk werden gemaakt'.
[223] Zie voor voorbeelden en jurisprudentie Maeyaert 2008, p. 449. Wanneer de spullen niet toebehoren aan de veroordeelde kan de eigenaar deze recupereren op grond van artikel 43bis Sw door een civiele vordering in te stellen.
[224] Zie o.m. Gent 7 mei 2008, Nullum Crimen, m.nt. M.C. Janssens (Namaak Rolex).

geconcludeerd ten aanzien van het civiele recht, namelijk dat een betrouwbaar watermerk bewijs kan leveren om een verband te leggen tussen het bestand en de licentienemer.

3.5 Auteursrechtelijke bescherming van watermerken

Tot slot is er aandacht voor de juridische bescherming van watermerken tegen verwijdering uit digitale content. Als voorwaarde om als bewijs te kunnen dienen mag het watermerk niet uit de gastobjecten verwijderd zijn. De wijze waarop de beveiliging van het watermerk in de gastobjecten moet plaatsvinden is vooral een technische vraag. De juridische vraag is dan of het watermerk onder het bestaande regime voldoende juridische bescherming krijgt tegen het omzeilen en aantasten daarvan.

Met de opkomst van DRM in de jaren negentig nam ook vraag naar bescherming van technische voorzieningen toe.[225] Dit resulteerde onder meer in twee WIPO-verdragen en leidde uiteindelijk in 2001 tot artikel 6 en 7 van de Auteursrechtrichtlijn waarin de rechtsbescherming van technische voorzieningen en informatie over het beheer van rechten is opgenomen tegen het omzeilen of verwijderen, toevoegen of manipuleren van (elektronische) identificatiemiddelen.[226] Doel van deze richtlijn was onder meer om de digitale distributie te stimuleren door aan de vraag vanuit de industrie te voldoen om technische beschermingsmaatregelen ook juridische bescherming te bieden. Met deze regeling is een grondslag ontstaan die het mogelijk maakt juridisch op te kunnen treden tegen het omzeilen en verwijderen van technische middelen. Hierbij kan gedacht worden aan verwijdering en aan aanvallen die zich richten op het onleesbaar maken van het watermerk waardoor detectie niet meer mogelijk is.

In zowel Nederland als België betreft de bescherming van doeltreffende technische beveiliging (par. 3.5.1) en elektronische informatiebeveiliging (par. 3.5.2) een civiele handhaving en zijn deze regelingen in de Nederlandse auteurswet opgenomen in artikel 29a en 29b Aw en in België in artikel 79bis en 79ter Aw.[227] In Nederland is er met opzet voor

[225] De gedachte achter beschermingsmaatregelen is dat bescherming van de content een Guibault & Mom 2007, p. 19.

[226] WIPO Auteursrecht Verdrag (WCT) en het WIPO Verdrag inzake Uitvoeringen en Fonogrammen (WPPT) zijn beiden op 20 december 1996 getekend en namens de Europese Gemeenschap goedgekeurd (2000/278/EG) op 16 maart 2000 (PbEG L 089 van 11 april 2000 p. 6-7). Zie voor de onderlinge verhouding en het doel van de verdragen en de richtlijn o.m. het tweede hoofdstuk van het WODC-onderzoek over de evaluatie van de artikelen 29a en 29b. Richtlijn nr. 2001/29/EG van het Europees Parlement en de Raad van de Europese Unie van 22 mei 2001betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, PbEG L 167/010, 22 juni 2001. (Auteursrechtrichtlijn). Zie voor een uitvoerig historisch overzicht van de totstandkoming van de richtlijn, o.m. Koelman 2003 (diss) en Guibault e.a. 2007.

[227] In Nederland bij Wet van 6 juli 2004 tot aanpassing van de Auteurswet 1912, de Wet op de naburige rechten en de Databankenwet ter uitvoering van richtlijn nr. 2001/29/EG van het Europees Parlement en de Raad van de Europese Unie van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (PbEG L 167) in werking getreden op 1 september 2004. In België bij Wet van 30 jhet iuni 1994 betreffende het auteursrecht en de naburige rechten. (BS 27.07.1994). Artikel 79bis is , ingevoegd bij W 2005-05-22/33, art. 26 en inwerking getreden op 27 mei 2005 en gewijzigd bij W 2008-06-08/31, art. 36, 2°, 012 en inwerkinggetreden op 26 juni 2008. Artikel 79ter is ingevoegd bij W 2005-

gekozen om deze handelingen als civielrechtelijk onrechtmatig aan te duiden en de strafrechtelijke sancties uit de auteurswet te laten. Een strafrechtelijke sanctie kan in Nederland slechts worden gevonden in artikel 32a Aw waarin een regeling is opgenomen met betrekking tot decodeermiddelen voor computerprogrammatuur dan wel in het commune strafrecht.[228] In België is overtreding van beide artikelen wel strafbaar gesteld in artikel 81 Aw.[229] In deze paragraaf wordt onderzocht of het watermerk juridische bescherming geniet onder de hiervoor besproken regelingen.

Het Hof van Justitie EU deed op 14 januari 2014 uitspraak in de zaak Nintendo/PC Box waar het Hof nader in gaat op het begrip 'doeltreffende technische voorziening'.[230] In navolging van A-G Sharpston komt het Hof tot de conclusie dat enkel rechtsbescherming wordt toegekend voor technische voorzieningen waarmee ten aanzien van werken wordt voorkomen of onmogelijk wordt gemaakt dat er geen handelingen worden verricht waarvoor toestemming van de auteursrechthebbende is vereist. Daarbij merkt het Hof tevens op dat deze voorzieningen geschikt moeten zijn om dit doel te verwezenlijken en niet verder mogen gaan dan daartoe noodzakelijk is.[231]

3.5.1 Omzeilen van technische voorzieningen

3.5.1.1 Nederland

Artikel 29a Aw maakt duidelijk dat degene, die kort gezegd een doeltreffende technische voorziening omzeilt of dergelijke omzeilingsdiensten verleent, producten daartoe levert of promoot, onrechtmatig handelt.[232] De twee belangrijkste bestanddelen zijn als definitie in de wet opgenomen en letterlijk overgenomen uit de richtlijn. Onder technische voorzieningen wordt verstaan 'technologie, inrichtingen of onderdelen die in het kader van hun normale werking dienen voor het voorkomen of beperken van handelingen ten aanzien van werken, die door de maker of zijn rechtverkrijgenden niet zijn toegestaan'.[233] Volgens de Memorie van Toelichting (hierna: MvT) kunnen niet alleen encryptiemethoden, maar kan elke kopieerbeveiliging op welke wijze die ook het beoogde effect bereikt rekenen op bescherming

05-22/33, art. 27 en inwerking getreden op 27 mei 2005. Zie verder artikel 81 voor de strafbaarstelling en 87bis inzake de vorderingen.

[228] Hierbij kan worden gedacht aan o.m. computervredebreuk (art. 138a Sr). Listig gebruik telecommunicatiediensten (art. 326c Sr) or manipuleren van gegevens (art. 350a Sr). Zie o.m Guibalt e.a 2007, p. 75 (part II).

[229] Zie ook par. 3.3.1.3. voor het verschil in benadering tussen Nederland en België.

[230] HvJ EU 23 januari 2014, zaak C-352/12, AMI 2014/2 m.nt. Koelman (Nintendo/PC Box).

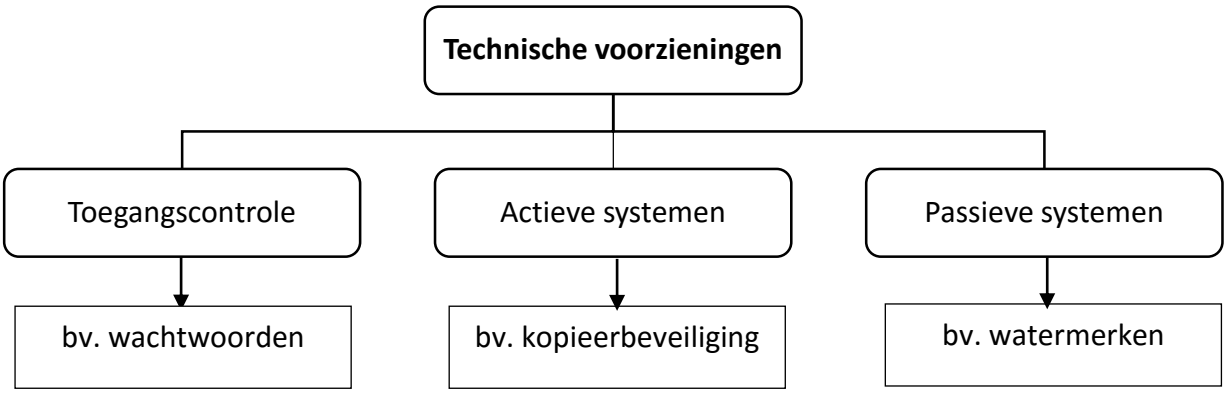
[231] Conclusie van A-G Sharpston van 19 september 2013 (ov. 53-63) voor HvJ EU 23 januari 2014, zaak C-352/12, ov. 31.

[232] Vgl. artikel 6 ARl.; art. 11 WIPO-verdrag inzake auteursrecht; artikel 18 van het WIPO-verdrag inzake uitvoeringen van kunstenaars en fonogrammen.

[233] Art. 29a lid 1. De toepassing op auteursrechtelijk beschermde werken houdt tevens in dat objecten die niet of niet langer auteursrechtelijk beschermd zijn geen beroep kunnen doen op deze bepaling. Zie ook de MvT (TK 2001–2002, 28 482, nr. 3, p. 55 en verder o.m. Spoor/Verkade/Visser 2005, p. 523; Koelman 2003 (diss.); Guibault & Mom 2007. Het kraken van beveiligingssystemen is hiermee op grond van dit artikel niet onrechtmatig maar kan dit wel op andere gronden zijn.

van artikel 29a Aw.[234] Deze technische voorzieningen zijn volgens de wet doeltreffend wanneer 'het gebruik van een beschermd werk door de maker of zijn rechtverkrijgenden wordt beheerst door middel van toegangscontrole of door toepassing van een beschermingsprocédé zoals encryptie, vervorming of andere transformatie van het werk of een kopieerbeveiliging die de beoogde bescherming bereikt'. De Nederlandse wetgever verduidelijkt zijn standpunten ten aanzien van deze definitie in de MvT door onder meer te stellen dat een voorziening niet 'doeltreffend' is wanneer het zonder bijzondere inspanning of door toeval te omzeilen is.[235] De MvT stelt ook dat het niet mag gaan om een voorziening waarvan slechts een signalerend of waarschuwend effect uitgaat.[236] Voor de toepassing van dit criterium is echter geen perfecte bescherming vereist. De vraag of een technische voorziening gekraakt is, komt op zichzelf geen zelfstandige juridische betekenis toe. Guibault en Mom stellen in de evaluatie van artikel 29a en 29b de voorzieningen centraal 'die de beoogde bescherming wel (kunnen) bereiken en controle over het gebruik van werken mogelijk maken (…), ook al zouden zij omzeild worden.'[237] Het is aan de rechter overgelaten om het begrip verder in te vullen.[238]

Noch uit de richtlijn noch uit de Nederlandse toelichting wordt duidelijk welke technische voorzieningen precies bescherming moeten toekomen. Guibault e.a. (2007) maken bij hun studie naar de effecten van de implementatie van de richtlijn in verschillende lidstaten een onderscheid tussen drie verschillende soorten van technische voorzieningen.[239]



Zij onderscheiden daarbij drie soorten: (1) technieken die toegangscontrole mogelijk maken; (2) actieve systemen die directe controle mogelijk maken ten aanzien van het gebruik, zoals kopieerbeveiliging en (3) passieve systemen die individuele informatie embedden met betrekking tot het werk en de rechthebbende (rightsowner) in staat stelt om deze identificeerbaar te maken in gevallen van inbreuk, waarbij zij watermerken expliciet

[234] MvT (TK 2001–2002, 28 482, nr. 3, p. 56-57).
[235] Dusollier 2005, p. 138; Guibault & Mom 2007, p. 6. Spoor/Verkade/Visser, p. 523; MvT (TK 2001–2002, 28 482, nr. 3, p. 57).
[236] MvT (TK 2001–2002, 28 482, nr. 3, p. 57).
[237] Guibault & Mom 2007, p. 6.
[238] MvT (TK 2001–2002, 28 482, nr. 3), p. 57. Zie daarvoor inmiddels ook HvJ EU 23 januari 2014, zaak C-352/12, AMI 2014/2 m.nt. Koelman (Nintendo/PC Box).
[239] Guibault e.a. 2007, p. 12. Ontleend aan Guibault en Mom 2007 (p. 20) in de nationale evaluatie.

noemen.[240] Het is in dit laatste geval niet duidelijk of zij hiermee watermerken bedoelen die als doel hebben bewijs te leveren wie de rechthebbende is en op grond daarvan de inbreuk aan te tonen of dat zij ook watermerken met een traitor tracingsdoel bedoelen. Beide toepassingen dienen als repressief en passief controlemiddel en vallen naar hun aard dan ook in deze categorie. In hun evaluatie kennen Guibault e.a. aan het begrip watermerken verschillende functies toe. Daarbij is niet altijd duidelijk welke toepassing van het watermerk zij voor ogen hebben.[241] Watermerken kunnen immers worden gebruikt voor kopieerbeveiliging, maar ook als doel hebben om de rechthebbende of de licentienemer te identificeren. Dat het enig verschil maakt mag duidelijk zijn. Watermerken die dienen ter kopieerbeveiliging zullen zonder enige twijfel onder de eerder genoemde wettelijke definities van artikel 29a vallen.[242]

In de wetsevaluatie van artikel 29a en 29b Aw plaatsen zij de actieve en passieve systemen en daarmee 'watermerken' in de hoek van informatiebeheer (art. 29b). Zij lijken daarmee een toepassing van artikel 29a uit te sluiten. Spoor/Verkade/Visser merken terecht op dat watermerken dat gericht is op de werking van apparatuur een overlap kan hebben met artikel 29a Aw.[243] Of watermerken een technologische voorziening is die onder de wettelijke definitie valt hangt af van de vraag of technologieën, die primair een controlefunctie hebben en technisch gezien niet primair gericht zijn op het voorkomen of beperken van onrechtmatige handelingen ten aanzien van werken, ook onder deze definitie vallen.[244] Guibault & Mom lijken dit niet mogelijk te achten doordat zij passieve systemen, waar ook watermerken onder vallen, van de toepassing van artikel 29a uitsluiten. Dat lijkt in lijn met de wetgever die ook in de MvT duidelijk spreekt over kopieerbeveiliging en in de wettekst duidelijk kiest voor het voorkomen of beperken van onrechtmatige handelingen. Het Hof van Justitie EU lijkt de elementen 'voorkomen of beperken' nader in te vullen door erop te wijzen dat enkel rechtsbescherming wordt toegekend voor technische voorzieningen waarmee ten aanzien van werken wordt voorkomen of onmogelijk gemaakt dat er geen handelingen worden verricht waarvoor toestemming van de auteursrechthebbende is vereist.[245] De nationale wetgever kiest, zoals eerder duidelijk werd, voor technologieën die meer doen dan waarschuwen en daarmee lijken technologieën die enkel controle achteraf mogelijk maken te zwak om voor bescherming in aanmerking te komen. De term 'beperken' had voor de uitspraak van het Hof van Justitie EU nog de mogelijkheid geboden om watermerktechnieken die controle achteraf mogelijk maken onder deze regeling te krijgen. In navolging van Struik, Van Schelven & Hoorneman zou men dan een ruime bescherming moeten toekennen aan 'technologie die tracht te voorkomen dat het werk door iemand anders dan de gebruiksgerechtigde wordt

[240] Guibault & Mom 2007, par. 4.1, p. 20 (figuur 1). Zie ook Guibault 2007, p. 13.
[241] Zie par. 2.2.4.
[242] Zie ook HvJ EU 23 januari 2014, zaak C-352/12 AMI 2014/2 m.nt. Koelman, ov. 28.
[243] Zie ook Spoor/Verkade & Visser 2005, par. 11.36, p. 525. Zie ook MvT (TK 2001–2002, 28 482, nr. 3, p. 60). Wanneer het een zaak betreft waarbij de informatie is verwijderd of gewijzigd en zowel artikel 29a als artikel 29b van toepassing kan worden geacht, dan heeft de gelaedeerde de keuze.
[244] Westkamp 2007, p. 52-53 stelt in deel II van de 'The Implementation of Directive 2001/29/EC in the Member States' ook de vraag of technologie die tot doel heeft de identiteit van de rechthebbende vast te stellen een hierbedoelde technologie kan zijn. Hij laat de vraag verder onbeantwoord.
[245] HvJ EU 23 januari 2014, zaak C-352/12 AMI 2014/2 m.nt. Koelman. Vgl. ov 28 en 31.

gebruikt'. In dat geval kan ook preventie een belangrijke rol spelen.[246] Dat het Hof enkel rechtsbescherming toekent voor technische voorzieningen waarmee ten aanzien van werken wordt voorkomen of onmogelijk gemaakt dat er kort gezegd onrechtmatige handelingen kunnen worden verricht is in het licht van de richtlijn logisch. Een andere interpretatie zou kunnen leiden tot een veel breder bereik waardoor ook over de beperkingen daarvan opnieuw zou moeten worden nagedacht. Dat is in beginsel vooral aan de 'wetgever'.

3.5.1.2 België

Artikel 79bis Aw stelt in § 1, dat 'eenieder die een doeltreffende technische voorziening omzeilt en dat weet of redelijkerwijs behoort te weten en die weet of redelijkerwijs behoort te weten dat deze omzeiling het plegen van inbreuken bedoeld in artikel 80 Aw kan vergemakkelijken, schuldig is aan een misdrijf (...). Technische voorzieningen worden tevens gedefinieerd als 'technologie, inrichtingen of onderdelen die in het kader van hun normale werking dienen voor het voorkomen of beperken van handelingen ten aanzien van werken of prestaties, die door de houders van auteursrechten of naburige rechten niet zijn toegestaan'. En technische voorzieningen worden volgens hetzelfde artikel 'geacht doeltreffend te zijn (…) indien het gebruik van een werk of prestatie wordt beheerst door de rechthebbende, door toepassing van een controle op de toegang of een beschermingsprocédé zoals encryptie, versluiering of andere transformatie van het werk of prestatie of een kopieerbeveiliging die de beoogde bescherming bereikt.'[247] Voor de bescherming op grond van dit artikel moet het watermerk een doeltreffende voorziening zijn. Ten aanzien van de technische voorziening lijkt de wetgever, overeenkomstig de richtlijn, vooral oog te hebben voor middelen die het gebruik van werken die door de auteurswet niet zijn toegestaan, voorkomt of beperkt. Ook de Memorie van Toelichting verwijst expliciet naar de toegang tot het werk, het gebruik van het werk of van een andere beschermde zaak die wordt geregeld door toepassing van een toegangscode. De wet beschermt verder elk ander soort beschermingsprocédé dat de beschermingsdoelstelling bereikt op een operationele en betrouwbare wijze, met toestemming van de rechthebbende voor de gebruiker.[248] De daarachterliggende doelstelling is volgens de wetgever dan ook dat men enkel 'ernstige' beveiligingsvoorzieningen wenst te beschermen. De wetgever lijkt door de toevoeging van ernstige beveiliging vooral oog te hebben voor technologieën waarbij gebruikers weinig andere keuze hebben, zoals bij toegang en actieve systemen. De rechthebbende lijkt hiermee, evenals naar Nederlands recht (vgl. art. 29a Aw), geen beroep te kunnen doen op artikel 79ter Aw voor de bescherming van watermerk-technieken met een traitor tracingsdoel. Watermerktechnieken met een traceerdoel zijn in die zin veel minder ernstig. Zij geven de eindgebruiker alle ruimte, en controle is alleen na overtreding mogelijk. Dat ligt anders voor toepassingen van watermerken, zoals bij de

[246] Struik, Van Schelven & Hoorneman 2010, p. 296.
[247] Vgl. art. 6 lid 3 Rl. Zie in dezelfde lijn A-G Sharpston voor HvJ EU 23 januari 2014, zaak C-352/12, AMI 2014/2 m.nt. Koelman (Nintendo/PC Box) .
[248] MvT bij de het wetsontwerp van 17 mei 2004 houdende de omzetting in Belgisch recht van de Europese richtlijn 2001/29/EG van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (DOC 51 1137/001), p. 25.

kopieerbeveiliging. Zij zullen deze bescherming zonder meer verdienen. Het is mede door een gebrek aan relevante jurisprudentie in het algemeen lastig te stellen of watermerken wel of geen bescherming toekomt op basis van artikel 79bis Aw. Op basis van de uitspraak door het Hof van Justitie EU in de Nintendo zaak lijkt het echter niet waarschijnlijk dat het watermerk met een traitor tracingsdoel bescherming geniet op grond van artikel 79bis Aw. Naar Nederlands recht is dat niet anders.

3.5.2 Bescherming van elektronische gebruiksinformatie

3.5.2.1 Nederland

In artikel 29b Aw wordt de wettelijke bescherming van elektronische gebruiksinformatie geregeld door het verwijderen, toevoegen of manipuleren van (elektronische) identificatiemiddelen als onrechtmatig aan te duiden.[249]
In het eerste lid wordt de handeling onrechtmatig geacht van 'degene die opzettelijk en zonder daartoe gerechtigd te zijn elektronische informatie betreffende het beheer van rechten verwijdert of wijzigt, of werken van letterkunde, wetenschap of kunst waaruit op ongeoorloofde wijze dergelijke informatie is verwijderd of waarin op ongeoorloofde wijze dergelijke informatie is gewijzigd, verspreidt, ter verspreiding invoert, uitzendt of anderszins openbaar maakt, en weet of redelijkerwijs behoort te weten dat hij zodoende aanzet tot inbreuk op het auteursrecht, dan wel een dergelijke inbreuk mogelijk maakt, vergemakkelijkt of verbergt'. Het gaat volgens de wettelijke en uit de richtlijn overgenomen definitie om 'alle door de maker of zijn rechtverkrijgenden verstrekte informatie welke verbonden is met een verveelvoudiging van een werk of bij de openbaarmaking van een werk bekend wordt gemaakt, die dient ter identificatie van het werk, dan wel van de maker of zijn rechtverkrijgenden, of informatie betreffende de voorwaarden voor het gebruik van het werk, alsmede de cijfers of codes waarin die informatie is vervat'. De gedachte achter deze bepaling kan volgens de minister gevonden worden in de behoefte in de digitale omgeving aan betrouwbare identificatie van beschermd materiaal, rechthebbende en licentievoorwaarden (beheersinformatie).[250] De zinsnede dat het dient ter identificatie van het werk dan wel zijn rechtsverkrijgende maakt duidelijk dat watermerken die dienen om de licentienemer bij overtreding op te kunnen sporen ook onder de definitie van dit artikel vallen. In de praktijk kan veel twijfel worden weggenomen door de code ook te laten verwijzen naar beheersinformatie waarover geen twijfel is, namelijk de gegevens van de rechthebbende. Een verwijdering of aantasten van de code levert daarmee altijd en zonder twijfel een inbreuk op ex. art. 29b Aw.

Artikel 29b Aw acht alleen het opzettelijk aanbieden van omzeilings- of verwijderingsmiddelen en verspreiden van versies waaruit de betreffende informatie is verwijderd onrecht-

[249] Deze bepaling is een vrijwel letterlijke vertaling van artikel 7 ARl en artikel 12 van het WIPO verdrag inzake auteursrecht en artikel 19 van het WIPOverdrag inzake uitvoeringen van kunstenaars en fonogrammen..
[250] MvT (TK 2001–2002, 28 482, nr. 3, p. 31).

matig. Hiermee maakt de wetgever een onderscheid tussen aanvallen die het watermerk ondervindt bij normaal gebruik en malafide aanvallen.

Aangezien er geen beroep kan worden gedaan op artikel 29a Aw vindt het watermerk zijn bescherming enkel nog in de strafbepaling van artikel 32a Aw. In dit artikel speelt het doel van de dader een belangrijke rol. Dit betreft in beginsel een strafrechtelijke bepaling, waarin ook een civielrechtelijke norm kan worden gelezen die tot een civielrechtelijke onrechtmatige daad (6:162 BW) kan leiden.[251] Voor alle technische voorzieningen geldt dat de inzet daarvan dient plaats te vinden binnen de grenzen van het recht, waaronder de bescherming van de persoonlijke levenssfeer (ov. 57 ARl.).

Het watermerk wordt uiteindelijk door artikel 29b Aw beschermd tegen verwijdering en manipulatie evenals tegen het ter beschikking stellen van middelen die dat mogelijk maken. De toepassing van dit artikel maakt het gebrek aan toepasselijkheid van artikel 29a Aw niet langer relevant. Het watermerk met een traitor tracingsdoel valt naar zijn aard tussen beide regimes in. Het watermerk kan eenvoudig toepassing vinden als beheersinformatie waardoor artikel 29b Aw van toepassing is. Hierdoor krijgt met name de rechthebbende bescherming ten aanzien van het middel dat hij inzet. Vanwege de bescherming die het watermerk verkrijgt onder artikel 29b Aw lijkt er voldoende juridische bescherming te zijn. Dat laat onverlet dat in de praktijk de regeling nauwelijks wordt gebruikt.[252] Sinds de inwerkingtreding van de artikelen 29a en 29b Aw zijn er slechts enkele rechterlijke uitspraken gedaan in verband met de bescherming van technische voorzieningen, terwijl de rechter zich nog niet éénmaal heeft uitgesproken in een procedure inzake de bescherming van informatie over het beheer van rechten.[253] Het is zonder specifiek onderzoek lastig aan te geven welke betekenis hier aan moet worden toegekend. Betekent dit dat de bescherming niet effectief is of juist wel?[254] De betekenis van deze bepalingen lijkt vooral te liggen in de boodschap die eruit bestaat dat het niet is toegestaan en dat in voorkomende gevallen er in ieder geval een beroep op kan worden gedaan. Juridisch gezien is het systeem daarmee gesloten. In de praktijk is het duidelijk dat de technische voorzieningen worden omzeild en de beheersinformatie wordt verwijderd. De prioriteiten lijken ook voor rechthebbenden hier niet primair te liggen. De beperkte middelen worden thans ingezet voor de bestrijding van de aanbieders en deze richt zich niet op het

[251] Zie Spoor/Verkade/Visser 2005, p. 539; Vzr Rb. Breda 24, April 2002, ECLI:NL:RBBRE:2002:AE1864; AMI 2002/14, p. 137 m.nt. Seignette; CR 2002, 235 m. nt. A.P. Meijboom; IER 2002, p. 50 m. nt. MdCB; (Brein/Lebbink; Modchips voor PS-consule). Zie voor de verhouding tussen artikel 29a en 32a verder o.m. de noten onder Rb. 's-Gravenhage 21 juli 2010, ECLI:NL:RBSGR:2010:BN1963, CR 2010, 179 m.nt. R.A. Overbeek, AMI 2011, p. 14 m.nt. Koelman (Nintendo/Webwinkels).

[252] Zie de evaluatie van artikel 29a en b Aw door Mom & Guibault 2007.

[253] Guibault en Mom (2007, p. 14) komen ook in hun onderzoek tot deze conclusie. In de periode na dit onderzoek is deze situatie niet veranderd. De voorlopig laatste uitspraak dateert van de Rb. 's-Gravenhage 21 juli 2010, ECLI:NL:RBSGR:2010:BN1963, CR 2010, 179 m.nt. R.A. Overbeek, AMI 2011, p. 14 m.nt. Koelman (Nintendo/Webwinkels). Geen enkele uitspraak had betrekking op watermerken of gelijkende technologie.

[254] Mijn inschatting zou zijn dat de mensen die in staat zijn technologische middelen aan te tasten zich niet laten weer houden, mede vanwege de geringe pakkans.

verwijderen van technische voorzieningen of beheersinformatie maar op het platform dat de content aanbiedt.[255] Deze strategie lijkt bij die keuze ook de meest vruchtbare.

3.5.2.2 België

Artikel 79ter Aw beschermt de informatie betreffende het beheer van rechten, die in § 2 wordt omschreven als 'alle door de rechthebbenden verstrekte informatie op grond waarvan het werk of prestatie, dan wel de auteur of andere rechthebbenden kunnen worden geïdentificeerd. Deze term wijst ook op informatie betreffende de voorwaarden voor het gebruik van het werk of prestatie, als ook op de cijfers en codes waarin die informatie vervat ligt.'[256] De vraag is of onder de term rechthebbende ook de licentienemer moet worden verstaan. Wanneer dit niet het geval is zou kunnen worden betwist of het opnemen van informatie met betrekking tot de licentienemer ook onder deze definitie valt. Dat zou in de praktijk overigens eenvoudig kunnen worden opgelost door in de code niet alleen informatie over de licentienemer maar ook over de licentiegever (auteursrechthebbende) op te nemen. Guibault e.a. 2007 classificeren in hun studie naar effecten van de richtlijn het watermerk met een identificatiedoel als een technische voorziening die het beheer van rechten regelt. Aangenomen mag worden dat het watermerk in ieder geval bescherming geniet onder toepassing van artikel 79ter Aw. Hiermee geniet het watermerk bescherming tegen verwijdering en manipulatie evenals tegen verspreiding van middelen die dat mogelijk maken. Ook in België is er weinig aandacht voor de bescherming van technische voorzieningen als bedoeld in beide artikelen. De wet biedt de mogelijkheid om juridische bescherming in te roepen. Het is vervolgens aan de rechthebbende om hier een beroep op te doen.

3.5.3 Tussenconclusie

In zowel Nederland als België is de Europese richtlijn die de bescherming van technische voorzieningen mogelijk maakt geïmplementeerd in nationale wetgeving. Zowel op basis van nationale wetgeving als inmiddels door een uitspraak van het Hof van Justitie in de zaak Nintendo/PC box is het niet aannemelijk dat aan het watermerk rechtsbescherming wordt toegekend als een doeltreffende technische voorziening als bedoeld in artikel 6 van de auteursrechtrichtlijn. In beide landen vindt het watermerk wél juridische bescherming in de artikelen in de auteurswet die elektronisch informatie beschermen. Het belangrijkste verschil is dat in België watermerken zowel via de civiel als strafrechtelijke weg beschermd worden terwijl in Nederland er geen strafrechtelijke bepaling is die dezelfde bescherming biedt.

[255] Zie par. 3.3.2.

[256] Artikel 79ter Aw: Een ieder die opzettelijk op ongeoorloofde wijze een van de volgende handelingen verricht: 1° de verwijdering of wijziging van elektronische informatie betreffende het beheer van rechten; 2° de verspreiding, de invoer ter verspreiding, de uitzending, de mededeling aan het publiek of de beschikbaarstelling voor het publiek van werken of van prestaties, waaruit op ongeoorloofde wijze elektronische informatie betreffende het beheer van rechten is verwijderd of waarin op ongeoorloofde wijze dergelijke informatie is gewijzigd, en die weet of redelijkerwijs behoort te weten dat hij zodoende aanzet tot een inbreuk op het auteursrecht of op een naburig recht, dan wel een dergelijke inbreuk mogelijk maakt, vergemakkelijkt of verbergt, is schuldig aan een misdrijf dat wordt bestraft overeenkomstig de artikelen 81 en 83 tot 86.

Hoewel er inhoudelijk kleine verschillen waarneembaar zijn, heeft dit geen effect op de bescherming van het watermerk in beide landen. Dit komt vooral omdat in beide landen er zelden een beroep op deze bepalingen wordt gedaan. Door het opnemen van bepalingen die tot doel hebben technologische voorzieningen te beschermen heeft het recht zijn plicht gedaan. Het probleem ten aanzien van de bescherming van deze voorzieningen ligt dan ook niet in de juridische beperkingen maar de bereidheid om dit recht te handhaven. De rechthebbende moet in de dagelijkse praktijk prioriteiten stellen en die liggen om begrijpelijke redenen elders.

3.6 Samenvatting en conclusie

Om als juridisch bewijsmiddel bij te kunnen dragen aan de handhaving van het auteursrecht is eerst onderzocht of het watermerk geaccepteerd zal worden door de afnemers van digitale content.

Watermerken maakt als techniek een onderdeel uit van het in de jaren negentig geïntroduceerde begrip Digital Rights Management dat in essentie niet meer dan een verzamelbegrip is voor het managen van gebruiksrechten van digitale informatiebronnen door een controlesysteem met technologische en organisatorische middelen. Bij het publiek heeft het begrip DRM een negatieve associatie gekregen door het gebruik van kopieerbeveiligingen die consumenten ook in hun legale handelingen beperkten. Dit had tot gevolg dat consumenten zich tegen producten met deze technische beveiliging keerden. Rechthebbenden die watermerken inzetten vermijden dan ook veelal de term DRM of presenteren deze als ‘social DRM’ waarbij de nadruk dan ligt op het gegeven dat watermerken consumenten feitelijk niet in hun handelen beperkt. Omdat watermerken anders dan bijvoorbeeld de kopieerbeveiliging de consument verder niet hindert in haar gebruik van het product is ook weinig reden om aan te nemen dat het watermerk niet door consumenten zal worden geaccepteerd.

Ten aanzien van de bijdrage die watermerken kunnen leveren aan de handhaving van het auteursrecht is gekeken naar de vraag wat consumenten ertoe brengt om content uit illegale bron te delen dan wel waarom zij dit achterwege laten. Als reden om het delen van auteursrechtelijk beschermde werken achterwege te laten geven zij onder meer de (dreiging van) morele en juridische kosten aan. Watermerken kunnen, mits er over de plaatsing ervan duidelijk wordt gecommuniceerd, in preventieve zin een appel doen op de morele en juridische kosten die gepaard gaan met onrechtmatig handelen. Hiermee is tevens duidelijk geworden dat het watermerk als preventiemiddel minder effectief zal blijken te zijn voor de groep die geen belang hecht aan morele en/of juridische kosten. In die zin is het watermerk vooral een middel om de groep ‘eerlijke’ consumenten, ‘eerlijk’ te houden.
Tevens is gekeken naar de vraag wie verantwoordelijk is voor de onrechtmatige verspreiding van content. Het antwoord op die vraag laat enerzijds zien hoe groot de groep is die aanvallen zal plegen op watermerken en anderzijds maakt het duidelijk hoe groot de groep is die

potentieel eerlijk kan worden gehouden met watermerken. Verschillende onderzoeken wijzen uit dat slechts een klein deel van bevolking (± 5%) verantwoordelijk is voor de onrechtmatige verspreiding van content. Een klein deel van deze groep ('the scene'), die bekend staat als los verband van goed georganiseerde groepen, beschikt over de kennis en kennissen om auteursrechtelijk beschermde werken, bij voorkeur vóór de officiële lanceerdatum, te verspreiden. Watermerken richten zich in dat licht op het eerlijk houden van bestaande gebruikers. Voor de beveiliging van watermerken betekent dit dat zij voldoende robuust moeten zijn om aanvallen van een kleine maar technisch vaardige groep te weerstaan. Er is, gezien de ervaringen bij andere technieken, weinig reden om aan te nemen dat watermerken niet gekraakt kunnen worden. Wanneer wij aannemen dat de werken niet eerder op het internet verschijnen dan dat de watermerken onklaar zijn gemaakt dan is de winst gelegen in de tijd tussen het op de markt brengen en de kraak voor producten waarbij de waarde het grootste is in het begin van hun levenscyclus, zoals bij een nieuwe film die in de (thuis)bioscoop wordt vertoond. Tot die tijd kan het in potentie een relatief grote groep weerhouden van het delen van de content. In die zin blijft, ook met het watermerk, de handhaving van auteursrechten op muziek, films en foto's een kat-en-muisspel.

Vervolgens is gekeken naar de vraag of het watermerk past in het handhavingsbeleid van de overheid en rechthebbenden. Watermerken moeten immers functioneren binnen de beleidskaders van zowel het overheidsbeleid als dat van particulieren handhavers. In Nederland en België zijn in de auteurswet mogelijkheden opgenomen om het auteursrecht zowel civiel als strafrechtelijke te handhaven. In Nederland geldt er een voorkeur voor civiele handhaving en is de strafrechtelijke handhaving in de praktijk heel lastig door een aanwijzing van het College van Procureurs waarin de voorkeur voor een civiele handhaving wordt bevestigd. In België bestaat er geen voorkeur en kan de rechthebbende zowel de burgerlijke als de strafrechtelijke weg bewandelen door in het laatste geval aangifte te doen. De handhaving van het auteursrecht is daarmee in beide landen in de eerste plaats een aangelegenheid van rechthebbenden. De (auteurs)wet maakt verder geen onderscheid tussen degenen tegen wie de rechthebbende zijn rechten wil handhaven. Door een mix van collectief georganiseerde en individuele rechthebbenden kan er niet worden gesproken van één privaat handhavingsbeleid. Collectief georganiseerde rechthebbenden richten zich in beginsel niet op individuele consumenten die weleens een werk up- of downloaden. Zij richten zich op individuen of groepen die onrechtmatig en op grote schaal werken uploaden en/of aanbieden. Individuele rechthebbenden bekijken vaak per geval of zij handhavend gaan optreden of niet. Of zij optreden tegen individuele consumenten hangt af van een groot aantal factoren. Belangrijke factoren zijn vaak of zij andere inkomsten genereren en of zij om principiële reden tot handhaving over willen gaan. Het watermerk dat in dit onderzoek centraal staat is naar zijn aard vooral interessant voor rechthebbenden die bereid zijn om individuele consumenten aan te spreken of die het watermerk willen inzetten als preventieve maatregel. Het watermerk biedt immers enkel de mogelijkheid om een verband te leggen tussen één licentienemer en het op internet aangetroffen werk.

Daarna is gekeken naar de vraag welke rol het watermerk kan spelen bij het vaststellen van inbreuk op het auteursrecht, en is nagegaan wanneer er sprake is van inbreuk op het auteursrecht. De effectiviteit van het watermerk als juridisch bewijsmiddel wordt immers naast de technische mogelijkheden van het watermerk vooral bepaald door de rol die het krijgt in de context van het bewijsrecht. Zowel naar Nederlands als Belgisch recht geldt dat op basis van het bewijsrecht en het materiële recht wordt bepaald welke rol het watermerk als juridisch bewijsmiddel kan spelen bij het vaststellen van auteursrechtinbreuk.

Naar zowel Nederlands als Belgisch recht is sprake van inbreuk op het auteursrecht wanneer iemand zonder toestemming van de rechthebbende een auteursrechtelijk beschermd werk aan het publiek ter beschikking stelt, zonder dat hij een beroep kan doen op een wettelijke beperking. In de regel heeft de consument geen toestemming gekregen voor het beschikbaar stellen van deze werken op internet. De aangesproken partij zal zelf een beroep moeten doen op de wettelijke beperkingen zoals het citaatrecht. Het proces van watermerken kan daarmee vergaand geautomatiseerd worden uitgevoerd door na het vinden van de vermeend inbreukmakende werken het watermerk te detecteren en te koppelen aan de gegevens van de licentienemer. Hierna zou er zelfs voor kunnen worden gekozen om geautomatiseerd de licentienemer aan te schrijven.

Zowel in Nederland als in België sluit men in het strafrecht aan bij de civielrechtelijke begrippen van respectievelijk openbaarmaking (mededelen aan het publiek) en verveelvoudiging (reproductie). In beide landen zijn hier strafrechtelijke elementen aan toegevoegd die zien op de wil van de dader in termen van opzet of een redelijk vermoeden (Nederland) of van kwaadwillig of bedrieglijk (België). Het watermerk kan geen van de hiervoor genoemde criteria invullen. Op grond van het materiële recht kan worden geconcludeerd dat zonder nader bewijs, de rechthebbende met het watermerk niet in staat is om bewijs te leveren voor alle elementen die nodig zijn om inbreuk op het auteursrecht vast te stellen. Het watermerk kan als bewijs dan enkel dienen om een verband aan te tonen tussen het bestand en de licentienemer.

Tot slot is er gekeken naar de vraag of het watermerk als technisch middel bescherming kan vinden in het recht. Het omzeilen van een watermerk lijkt op grond van Nederlandse en Belgische wetgeving in beginsel niet onrechtmatig. Het verwijderen van beheersinformatie zelf uit een versie is wel onrechtmatig. In Nederland blijft het aanbieden van omzeilings- of verwijderingsmiddelen in ieder geval via de weg van artikel 32a Aw wel verboden. Hierin is echter ook een civielrechtelijke norm te lezen die tot een civielrechtelijke onrechtmatige daad (6:162 BW) kan leiden, waardoor weliswaar via een omweg het aanbieden van deze middelen toch onrechtmatig is. De effectiviteit van deze beschermingsmaatregelen blijft onduidelijk. Wetsevaluaties in Nederland laten in ieder geval zien dat er weinig gebruik wordt gemaakt van deze regelingen. In hoeverre deze maatregelen een preventieve werking hebben is ook niet duidelijk. De kleine deskundige groep die verantwoordelijk is voor de verspreiding van content en deze technische voorziening buiten werking stelt laat zich in de praktijk in ieder geval niet door deze bepalingen afschrikken. Het probleem dat zich hier voordoet ligt meer in

het domein van de handhaving van de regels dan in het gebrek daaraan. De rechthebbende moet in de dagelijkse praktijk prioriteiten stellen en die liggen - terecht - elders. Het voorgaande leidt in ieder geval tot de conclusie dat men zich bij watermerken beter kan richten op een betere technische beveiliging dan een betere juridische beveiliging. Want andere wetgeving zal waarschijnlijk niet tot betere resultaten zal leiden.

Samenvattend is er weinig reden om aan te nemen dat het watermerk niet door gebruikers van content zal worden geaccepteerd. Het in beginsel onzichtbare watermerk zal, wanneer de aanwezigheid duidelijk wordt gecommuniceerd, als preventief middel effectief zijn bij die groep mensen die vanwege de morele en juridische kosten afzien van onrechtmatig handelen. Het watermerk dat naar haar aard gericht is op het leggen van een verband tussen de licentienemer en het op internet aangetroffen bestand past bij het beleid van de overheid en individuele rechthebbenden. Hoewel deze beide actoren in beginsel terughoudend zijn bij het aanspreken van individuele inbreukmakers brengt de aard van het watermerk met zich mee dat zij voor de effectiviteit van het watermerk wel bereid moeten zijn de licentienemer aan te spreken wanneer deze het werk onrechtmatig op internet plaatst. Op grond van het materi materiële recht kan worden geconcludeerd dat het watermerk als bewijs enkel kan dienen om een verband aan te tonen tussen het bestand en de licentienemer.

4 Watermerken als bewijs in een juridische procedure

'In God we trust, all others bring data.'[1]

4.1 Inleiding

In de vorige hoofdstukken is duidelijk geworden dat een betrouwbaar watermerk als technisch bewijsmiddel vanuit een materieelrechtelijk perspectief enkel kan bijdragen aan het bewijs door een verband te leggen tussen het op internet aangetroffen bestand en de vermeende licentienemer (hierna: licentienemer).[2] Voorts is duidelijk geworden dat het watermerk slechts kan bijdragen aan bewijs door aan te tonen dat de licentienemer het bestand openbaar heeft gemaakt. Binnen die context kan het watermerk slechts bijdragen aan het bewijs van de stelling dat het op internet aangetroffen bestand bij de licentienemer hoort.

In dit hoofdstuk wordt vanuit het bewijsrecht nader ingegaan op de vraag of het watermerk in een juridische procedure een effectief bewijsmiddel kan vormen voor het feit dat het bestand bij de licentienemer hoort.[3] Het watermerk is effectief wanneer de rechter dat feit bewezen kan achten. In het licht van dit onderzoek is het van belang om zicht te krijgen op de vraag hoe het bewijsrecht werkt op punten die voor de waardering van watermerken van belang zijn.

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te kunnen beoordelen is het noodzakelijk om, naast het materiële recht (hoofdstuk 3), het watermerk in de context van het bewijsrecht te plaatsen. De effectiviteit van bewijsmiddelen wordt daar beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en de stellingen die ten aanzien van dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd.[4] Uiteindelijk wordt in dat samenstel van regels bepaald in hoeverre het watermerk effectief is in relatie tot het te bewijzen feit dat het bestand toebehoort aan de licentienemer.

Vanuit dit perspectief is het vooral van belang om aandacht te besteden aan de vraag welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren ten aanzien van het gestelde feit en het watermerk als bewijsmiddel. En de wijze waarop de rechter deze stellingen beoordeelt. Deze vragen worden zowel naar Nederlands als Belgisch civiel en strafrecht onderzocht. Per land en rechtsgebied is ten eerste gekeken naar de bewijsrisco-verdeling tussen partijen. Het gaat daarbij om de vraag welke stellingen partijen kunnen en

[1] W.E. Deming (1900-1993) in: Hastie, Tibshirani & Friedman 2012, p. vii.
[2] Of er sprake is van een licentienemer zal blijken tijdens de procedure. In de procedure kan bijvoorbeeld blijken dat het watermerk vals is of dat de authenticatie niet goed verlopen is. Vanwege de leesbaarheid is er echter voor gekozen om de term licentienemer aan te houden. Zie ook par. 1.2.
[3] In het voorgaande hoofdstukken werd reeds duidelijk dat het watermerk verder niet kan bijdragen aan het bewijs. In dit hoofdstuk geldt steeds als uitgangspunt dat de gedaagde of verdachte (licentienemer) degene is die als licentienemer in het watermerk is opgenomen (par. 2.2.5) en dat het (audio, film of foto-)bestand zonder toestemming van de rechthebbende op internet is geplaatst (par. 3.4).
[4] In tegenstelling tot zowel het Nederlandse als Belgische civiele recht kan de verdachte in het Nederlandse en Belgische strafrecht ervoor kiezen om te zwijgen en zelf geen enkel verweer te voeren zonder dat het zwijgen in beginsel consequenties heeft voor het vaststellen van dat feit.

soms moeten aanvoeren en welke partij het risico draagt wanneer de feiten onduidelijk blijven. Ten tweede is aandacht besteed aan de meest aannemelijke verweren die de wederpartij kan voeren tegen het watermerk en het feit waarvoor het watermerk als bewijsmiddel wordt ingezet. Ten derde is gekeken naar de vraag hoe de rechter tot zijn bewijsoordeel komt en welke rol deskundigen daarbij spelen.

Als uitgangspunt bij de uitwerking van dit hoofdstuk is genomen dat partijen en de rechter volgens de regels van het bewijsrecht het feit proberen te bewijzen.[5] Dat heeft onder meer tot gevolg dat de hoofdlijnen van het bewijs worden weergegeven en bijvoorbeeld niet tot in detail wordt ingegaan op de vraag wanneer een partij nu exact zijn stelling voldoende heeft weergegeven.[6]

4.2 Beslissen over feiten naar Nederlands civiel recht

Als uitgangspunt van het Nederlands civiele (bewijs)procesrecht geldt dat partijen de omvang en inhoud van het geschil bepalen.[7] Het is aan partijen overgelaten om vorderingen in te stellen, stellingen aan te dragen, te onderbouwen en deze eventueel te bewijzen. De rechter is ten aanzien van de omvang en inhoud van het geschil in beginsel lijdelijk. Dat laat onverlet dat zowel rechters, wetgever als literatuur de laatste jaren actief inzetten op een actieve rol van de rechter.[8] Zijn taak is om het geschil te beslechten en in casu om te beslissen of het gestelde feit kan worden vastgesteld.

Om de procedure zo redelijk en efficiënt mogelijk te laten verlopen moeten partijen de rechter en elkaar zoveel en zo vroeg mogelijk in de procedure duidelijkheid verschaffen over het geschil (substantiëringsplicht).[9] Op beide partijen rust dan ook een informatie- en mededelingsplicht.[10]

---

[5] Het gaat hier anders gezegd om een intern perspectief hoe de rechter idealiter moet beslissen en niet om welke vrijheid hij heeft om tot een beslissing te komen.

[6] Zie voor een meer volledig overzicht van het bewijsrecht o.m. Asser 2013; Schwartzenberg 2013; Hidma & Rutgers 2004; Giesen 2001 (diss.). Zie meer specifiek voor elektronisch bewijs Van Stekelenburg 2009 (diss.) en voor een vergelijking met België o.m. Bosse 2003 (diss.). Zie voor een rechtsvergelijkend perspectief ten aanzien van fact-finding Verkerk 2010 (diss.).

[7] Het civiel bewijsrecht is hoofdzakelijk geregeld in het wetboek van Burgerlijke Rechtsvordering (art. 149-207 Rv). Het bewijsrecht is van toepassing op de hier bedoelde dagvaardingsprocedure in eerste aanleg inclusief verzetprocedure en hoger beroep (art. 353 lid 1 Rv) en voor zover toepasselijk in cassatie (art. 418a Rv). In kort geding is het bewijsrecht niet van toepassing.

[8] De rechter heeft en neemt in de praktijk wel enige vrijheid in zijn zoektocht naar de juridische waarheid. Zie o.m. Handelingen I 2010-2011, nr. 26 - p. 47. Zie over de lijdelijkheid van de rechter in relatie tot de waarheidsvinding meer uitgebreid De Bock 2011(diss.) en Asser 2013, p. 11. Zie ook rechters zelf op de themamiddag van het LOVCK “Geen plaats meer voor de lijdelijkheid van de rechter”(Wetzels 2011 p. 20). Zie ook HR 25 maart 2011, ECLI:NL:HR:2011:BO9675, NJ 2012/627 m.nt H.J. Snijders (Hoogte kinderalimentatie), ov. 3.3. De rechter mag ambtshalve oordelen dat partijen in strijd hebben gehandeld met de waarheidsplicht van art. 21 Rv. en daaraan, ook zonder dat partijen daarover specifiek hebben gedebatteerd, gevolgen verbinden die in overeenstemming zijn met de aard en de ernst van deze schending.

[9] Zie voor meer rechtsvergelijkend perspectief ook Verkerk 2010 (diss.), p. 376.

[10] Asser 2013, p. 40; Schwartzenberg 2013, p. 28. Vanwege zijn informatie- en stelplicht zal de eiser al in zijn dagvaarding de eerder door verweerder geuite pre-processuele verweren moeten vermelden, alsmede zijn reactie daarop inclusief bewijsmiddelen om deze te ondersteunen.

In het Nederlands civiel recht kan de rechter behoudens wettelijke beperkingen een feit bewezen achten op grond van zijn eigen overtuiging of op grond van feiten of omstandigheden van algemene bekendheid en algemene ervaringsregels.[11] Daarnaast heeft de wetgever twee gronden gegeven waarop de rechter een feit in een civiele procedure moet vaststellen.[12] Ten eerste moet de rechter feiten of rechten die door de ene partij zijn gesteld en door de wederpartij niet of niet voldoende zijn betwist, als vaststaand beschouwen.[13] Ten tweede brengt het systeem van de wet met zich mee dat de rechter feiten moet erkennen die door de ene partij zijn gesteld en door de andere partij zijn erkend.[14] In deze paragraaf zal de nadruk liggen op de situatie waarin de gedaagde het gestelde feit, dat het bestand aan hem toebehoort, betwist. Wanneer de gedaagde het feit erkent zal het watermerk immers geen rol meer spelen in de procedure.[15]

Het gaat dus om de vraag welke stellingen partijen moeten en redelijkerwijs kunnen aanvoeren ten aanzien van watermerken, en op welke wijze de rechter beslist over de feiten. Om die reden wordt eerst ingegaan op de bewijsrisicoverdeling (par. 4.2.1). Daarbij zal nader worden ingegaan op de vraag welke stellingen partijen dienen aan te voeren en welke mogelijkheden de rechter heeft om feiten vast te stellen en via de bewijslastverdeling het vaststellen van feiten zo eerlijk en efficiënt mogelijk te laten verlopen. Daarna wordt ingegaan op aannemelijke verweren die de gedaagde (licentienemer) kan aanvoeren om het watermerk ineffectief te maken (par. 4.2.2). Tot slot wordt gekeken naar de vraag hoe de rechter tot zijn bewijsoordeel komt (par. 4.2.3). De paragraaf wordt afgesloten met een tussenconclusie (par. 4.2.4).

4.2.1 Bewijsrisicoverdeling

Om de rechter de mogelijkheid te geven om tot een beslissing te komen heeft de wetgever ervoor gekozen om het risico dat de gestelde feiten in een procedure onduidelijk blijven, toe te delen aan de partij die de bewijslast voor dat feit draagt.[16] Vervolgens is in de rechtspraak uitgebreide jurisprudentie ontwikkeld ten aanzien van de bewijsrisicoverdeling.

Samengevat worden door partijen in een procedure stellingen aangevoerd en wordt bewijs aangeboden. Vervolgens geeft de rechter veelal een voorshands bewijsoordeel en eventueel verleent hij een bewijsopdracht of vraagt hij een deskundigenbericht. Partijen kunnen daarop reageren bijvoorbeeld doordat een partij in een contra-enquête het door de wederpartij geleverde bewijs probeert te ontzenuwen door het leveren van tegenbewijs of juist het tegen-deelbewijs levert. Tot slot geeft de rechter een definitief bewijsoordeel dat in dialoog met

[11] Art. 149 lid 2 Rv.
[12] Zie Asser 2013; Schwartzenberg 2013, p. 15.
[13] Art. 149 lid 1 Rv.
[14] Art. 154 j° art. 149, lid 1 Rv eerste zin.
[15] Zie bijv. vzr. Rb. Amsterdam 16 oktober 2008, ECLI:NL:RBAMS:2008:BG0972, ov. 4.7. waarin de gedaagde erkent dat zij gelegenheid biedt tot publicatie van foto's op haar website waarop auteursrecht van derden rust.
[16] Zie voor achtergronden van de bewijsrisicoverdeling o.m. Asser 2013, p. 301; Giesen 2001 (diss.).

partijen tot stand is gekomen. De bewijsbeslissing is daarmee tot stand gekomen binnen de ruimte die de stellingen van partijen hebben gelaten.

De wijze waarop de rechter tot het vaststellen van feiten komt kan in een aantal fasen worden onderverdeeld. In het navolgende worden drie fasen nader uitgewerkt.[17] De eerste fase ziet op het stellen en betwisten van stellingen door partijen (par. 4.2.1.1). Het is in deze fase aan de rechter om te oordelen of partijen voldoende hebben gesteld dan wel betwist. Indien hij tot dat oordeel komt zal de rechter in de volgende fase de bewijslastverdeling moeten vaststellen om te bepalen welke partij als eerste tot het leveren van bewijs wordt toegelaten (par. 4.2.1.2) Daarna treedt de fase in waarin partijen bewijs kunnen gaan leveren onder toezicht van de rechter in de vorm van een bewijsopdracht of doordat de rechter een deskundigenbericht vraagt (par. 4.2.1.3).

4.2.1.1 Stellen en betwisten

In de eerste fase is er in juridische zin nog geen sprake van het leveren van bewijs, maar dienen partijen hun stelling(en) voldoende concreet aan te brengen en te motiveren. Het onvoldoende stellen of betwisten van stellingen kan ertoe leiden dat de rechter de zaak direct afdoet en aan de fase van bewijslevering niet meer wordt toegekomen. In de praktijk worden veel zaken al beslist in de fase van stellen en betwisten.[18]

Stellen

Op de partij die een vordering instelt rust een stelplicht.[19] Om aan deze plicht te voldoen zal deze partij zijn stelling voldoende moeten onderbouwen, zowel ten aanzien van de wettelijke vereisten als de concrete feitelijke uitwerking daarvan.[20] Of er in kwestie voldoende is gesteld hangt samen met de kwaliteit van de betwisting ervan. Bij aanvang van de procedure rust de stelplicht in elk geval op de rechthebbende (eiser) die een vordering instelt tegen de licentienemer (gedaagde). Wanneer de rechthebbende onvoldoende stelt zal dit tot gevolg hebben dat de vordering in beginsel zal worden afgewezen wegens een gebrek aan feitelijke

[17] Zie voor een overzichtelijke en meer uitgebreide indeling in fasen onder meer Van den Brink 2008. Vanaf de eerste fase geldt dat voor de beoordeling van het bewijs de regels inzake toelaatbaarheid, bewijskracht en bewijswaardering van toepassing zijn. De verschillende fasen zijn overigens vooral begripsmatige hulpmiddelen.
[18] Zie o.m. Schwartzenberg 2013, p. 28; Van den Brink 2008, p. 94. Van der Brink bepleit dan ook dat wanneer rechters een feitelijke stelling als onvoldoende concreet onderbouwd willen afdoen zij zich moeten afvragen (en motiveren) wat die partij nog had kunnen en dus moeten doen. De Hek (2013, p. 109), raadsheer in het Hof Arnhem-Leeuwarden, vreest dat deze situatie alleen maar zal toenemen met de toenemende nadruk op Productienormen in de rechtspraak.
[19] Art. 149 tweede volzin Rv. Uit de toepasselijke regel van materieel recht die ten grondslag ligt aan de vordering zal duidelijk worden welke elementen nodig zijn om het ingeroepen rechtsgevolg teweeg te brengen, wat de concrete stelplicht inhoudt en welke partij de plicht heeft die feiten te stellen. Zie o.m. Schwartzenberg 2013, p. 24. Zie ten aanzien van de nadere materiële eisen ten aan zien van inbreuk op het auteursrecht par. 3.4. Later in de procedure geldt er ook een stelplicht voor die partij die een zelfstandig verweer voert.
[20] Zie o.m. Asser 2013, p. 310; Schwartzenberg 2013, p. 31; Van den Brink 2008, p. 91. De eiser moet niet alleen zorgen voor duidelijke stellingen maar bij het overleggen van producties ook aangegeven welke stelling hij daarmee onderbouwt (Schwartzenberg 2013, p. 24).

grondslag. Aan de vraag of het watermerk als juridisch bewijsmiddel kan worden gekwalificeerd komen we dan niet meer toe.

De rechthebbende zal mede vanwege zijn informatie- en stelplicht de rapportage ten aanzien van het watermerk direct in zijn stukken aanvoeren. Enerzijds om zijn stelling dat het op internet aangetroffen bestand aan de licentienemer toebehoort kracht bij te zetten. Anderzijds om te voldoen aan zijn stelplicht. De mate waarin een stelling moet worden onderbouwd of gemotiveerd is immers mede afhankelijk van de kennis die de andere partij (licentienemer) heeft over een bepaalde stelling.[21] Het ligt dan ook voor de hand dat de rechthebbende zijn stelling onderbouwt met andere relevante stukken. In de praktijk zal de rechthebbende het watermerk als bewijsmiddel ook al kenbaar hebben gemaakt in zijn eerste sommatiebrief waarin hij stelt dat de licentienemer inbreuk heeft gemaakt en dit gebruik moet staken. Ook voor de rechthebbende is immers een schikking de snelste oplossing van het geschil.

Betwisten

Feiten of rechten die door de ene partij zijn gesteld en door de andere partij niet of niet voldoende zijn betwist moet de rechter als vaststaand beschouwen.[22] Om te voorkomen dat het gestelde feit direct door de rechter wordt vastgesteld zal de gedaagde (licentienemer) het gestelde feit dan ook moeten betwisten.[23] Ook voor de betwisting geldt dat deze voldoende concreet onderbouwd moet zijn. Het antwoord op de vraag wanneer een feit voldoende gesteld en betwist is hangt samen met de kwaliteit van de stellingen. Hoe specifieker de ene partij zijn stelling formuleert en onderbouwt, hoe specifieker de andere partij moet zijn om diens stelling als 'voldoende' gekwalificeerd te krijgen.[24] In die zin is er sprake van een wisselwerking tussen de gebruikte stelling(en) en onderbouwing(en).[25] Het direct inbrengen van het watermerk als bewijsmiddel brengt daarmee tevens het praktische voordeel met zich mee dat de rechthebbende direct de lat heeft verhoogd voor de licentienemer om diens stelling te (kunnen) betwisten.[26]

Een in beginsel ongeloofwaardige stelling is voor de vaststelling van de feiten pas relevant als de wederpartij die stelling ook betwist. Wanneer de wederpartij deze stelling gemotiveerd betwist dan zal de andere partij nadere gegevens moeten verschaffen om aan zijn plicht te kunnen (blijven) voldoen.[27] Indien een partij er niet in slaagt de stelling voldoende te

[21] Zie o.m. Huydecoper 2002, p. 214; Schwartenberg 2013, p. 31.
[22] artikel 149 lid 1 tweede zin Rv.
[23] Art. 149 lid 1 Rv.
[24] Zie o.m. Asser 2013, p. 316; Schwartzenberg 2013, p. 31; Van den Brink 2008, p. 92
[25] Zie hierin ook de wisselwerking met de dagvaarding waarin de rechthebbende de preprocessuele verweren van de wederpartij moet opnemen. Deze verweren verzwaren in beginsel de stelplicht van de eiser.
[26] Zie meer over de kwalificatie van het watermerk als bewijsmiddel hoofdstuk 4 over toelaatbaar bewijs.
[27] Van een partij die met een onaannemelijke stelling komt, die gemotiveerd wordt betwist, mag worden verwacht hij met zoveel mogelijk gegevens komt om zijn stelling te onderbouwen. HR 8 juli 1992, NJ 1992, 713, zie ook A-G Koopmans voor het arrest; Van den Brink 2008, p. 92.

betwisten dan kan de rechter de stelling passeren op grond van het feit dat de stelling onvoldoende is betwist.[28]

Ten aanzien van watermerken kan de wisselwerking van stellen en betwisten er in de praktijk als volgt uitzien: De rechthebbende zal beginnen met de stelling dat er inbreuk is gepleegd door de gedaagde. Indien de gedaagde in zijn betwisting slaagt, ligt het voor de hand dat de rechthebbende zijn stellingen aanvult en onderbouwt met bewijs.[29] De rechthebbende kan vervolgens stellen dat een bestand is aangetroffen dat eerder aan de gedaagde is afgegeven. Ook dit feit zal de gedaagde moeten betwisten om te voorkomen dat het komt vast te staan. Het watermerk speelt tot nu toe eigenlijk nog geen rol. Het watermerk krijgt in dit voorbeeld pas een rol als de gedaagde het feit betwist door bijvoorbeeld te stellen dat meer mensen dat bestand hebben gekregen. Wanneer de rechthebbende vervolgens weer stelt dat het betreffende bestand een watermerk bevat dat naar hem wijst en de gedaagde deze stelling weer wil betwisten, komen vanaf dat moment de verweren ten aanzien van het watermerk centraal te staan.[30] De gedaagde kan bijvoorbeeld betwisten dat het bestand een watermerk bevat, dat het watermerk naar hem wijst (betrouwbaarheidsverweer), dat het watermerk rechtmatig is verkregen (toelaatbaarheidsverweer), of dat het bestand weliswaar naar hem wijst maar zonder zijn handelen op internet moet zijn gekomen (alternatieve verklaring). Ook voor deze verweren geldt dat de gedaagde de betwisting voldoende zal moeten onderbouwen. Wanneer de gedaagde het hiervoor gestelde feit niet betwist, is het watermerk effectief te noemen omdat het de rechter in staat heeft gesteld (het feit) vast te stellen dat het bestand aan de gedaagde (licentienemer) toebehoort. Het watermerk kan met andere woorden ook effectief zijn zonder dat de rechter de betrouwbaarheid van het watermerk ooit daadwerkelijk heeft onderzocht.[31]

Voor de beslissing of de feitelijke stelling kan worden vastgesteld zijn bewijsmiddelen met andere woorden weliswaar relevant, maar gelet op de stelplicht en betwisting dus niet geheel bepalend. Wanneer in voorkomend geval de rechthebbende onvoldoende stelt of de gedaagde het gestelde feit onvoldoende betwist komt de rechter niet toe aan een oordeel over het watermerk. De rechterlijke overtuiging ten aanzien van het watermerk is dan ook alleen van belang als de gedaagde betwist dat dat bestand daadwerkelijk naar hem wijst. Alleen dan hangt het bewijs geheel van het watermerk af.

[28] HR 12 mei 1989, NJ 1989, 596 (Dolmans/Wouters); Schwartzenberg 2013, p. 31. Asser 2013, p. 316.
[29] In de praktijk zullen partijen direct in de stukken zoveel mogelijk stellingen aanvoeren en onderbouwen, om te voorkomen dat de rechter de stellingen verwerpt als onvoldoende onderbouwd.
[30] Zie voor de meest aannemelijke verweren par. 4.2.2.
[31] De verklaring hiervoor dient voornamelijk te worden gevonden in het uitgangspunt dat partijen de omvang van het geschil bepalen. De rechter hoeft hier overigens niet lijdelijk te zijn en kan ingrijpen als het hem zeer onaannemelijk voorkomt, maar zal zich in het licht van het voorgaande niet snel hiertoe geroepen voelen.

Bewijsrechtelijke uitdagingen voor partijen ten aanzien van watermerken

Evenals in iedere andere procedure is het ook in zaken waarin watermerken als bewijs worden aangevoerd van belang dat partijen de nodige informatie kunnen verzamelen. Met het oog op het inschatten van de proceskansen en het verkrijgen van informatie dat als bewijs kan worden gebruikt heeft de wetgever het voor partijen ook mogelijk gemaakt om voorafgaande aan de hoofdprocedure informatie te verzamelen.[32]

De gedaagde kan tegen deze achtergrond dan ook informatie en inzicht verkrijgen in de wijze waarop de authenticatie tot stand is gekomen en de wijze waarop het watermerk aan het bestand is toegevoegd en uiteindelijk is gedetecteerd en uitgelezen.[33] De gedaagde zal een deel van deze informatie krijgen in de vorm van het verslag dat de rechthebbende inbrengt als bewijs. De rechthebbende is immers verplicht om inzage te verschaffen in de bewijsmiddelen die hij gebruikt om zijn eigen stellingen te onderbouwen.[34] Het instellen van een vordering tot afgifte van die stukken zal in de praktijk voldoende zijn. Het leggen van conservatoir bewijsbeslag om te voorkomen dat de stukken die de gedaagde wenst worden vernietigd lijkt mij weinig zinvol.[35] De rechthebbende die dat wil zal de betreffende gegevens immers vernietigen voordat hij de gedaagde aanschrijft. Waardoor tegen de tijd dat de gedaagde beslag wil leggen de gegevens al reeds vernietigd of verborgen zijn en beslag leggen weinig zin meer zal hebben.

De vraag is of de gedaagde ook recht heeft op de onderliggende documenten waarin bijvoorbeeld sleutels of andere vertrouwelijke informatie is opgenomen.[36] Gegevens die geen vertrouwelijk karakter hebben zal de rechthebbende, al dan niet op verzoek van de gedaagde, moeten aanleveren. Artikel 843a Rv biedt de gedaagde in dit geval de mogelijkheid om op zijn kosten inzage te vorderen in bepaalde bescheiden die de rechthebbende tot zijn

[32] Met tussenkomst van de rechter kunnen partijen vragen om een voorlopig getuigenverhoor (art. 186 e.v. Rv), deskundigenbericht, plaatsopneming, bezichtiging (art. 202 Rv), exhibitievordering (art. 843a Rv) en het bewijsbeslag (art. 1019b en c Rv). Zie ook Asser 2013, p. 195.

[33] In hoeverre partijen in Nederland technische verweren voeren is mij uit onderzoek onbekend. Van Buskirk & Lui 2006 constateerden dat door advocaten in de VS in (straf)zaken waarbij digitaal bewijs en experts werden ingezet nauwelijks gebruik werd gemaakt van de Daubertcriteria (authenticiteit, accuraatheid, betrouwbaarheid) om het bewijs aan te vechten. Kessler (2010, p. 9) merkt op dat er tot 2010 geen ander onderzoek is dat thans op andere conclusies zou wijzen. IT-Experts in Nederland gaven aan verzoeken van advocaten te krijgen om met rapporten mee te lezen of een contra-expertise uit te voeren maar het blijft de vraag hoe vaak dit voorkomt en uiteindelijk in de rechtszaal ook daadwerkelijk leidt tot het voeren van verweer. Het onderzoek kan immers ook betrouwbaar zijn gebleken in een contra-expertise.

[34] Zie art. 111, lid 3 Rv (dagvaarding), 128 lid 5 Rv (conclusie van antwoord) en art. 85 Rv. Vgl. verplichting van partijen om elkaar en de rechter volledig en naar waarheid te informeren (art. 21 Rv) en op bevel van de rechter de relevante bescheiden in het geding te brengen (art. 22 Rv). Wanneer een partij dit nalaat kan de rechter de gevolgtrekking maken die hij geraden acht, bijvoorbeeld door de stellingen of het bewijsaanbod van de betreffende partij te passeren.

[35] Art. 843a Rv biedt in verbinding met art. 730 Rv wel voldoende grondslag voor het leggen van (conservatoir) bewijsbeslag in niet-IE-zaken. Zie HR 13 september 2013, ECLI:NL:HR:2013:BZ9958, IER 2014/9, m.nt. F.W.E. Eijsvogels, JOR 2013/330, m.nt. E. Loesberg (Molenbeek Invest/Begeer c.s.), ov. 3.6.1.

[36] De werking van het watermerksysteem moeten reeds blijken uit het verslag dat de rechthebbende als bewijsmiddel aanvoert.

beschikking heeft.[37] Indien nodig kan de rechter bepalen op welke wijze de inzage, afschrift of uittreksel zal worden verschaft.[38] Op de hoofdregel om tot verstrekking van deze gevraagde gegevens over te gaan bestaan twee relevante uitzonderingen.[39]

Ten eerste kan in dit geval de rechthebbende evenals ten aanzien van de meer algemene exhibitiebepaling van artikel 22 Rv een gewichtige reden hebben om een exhibitie te weigeren.[40] In dit geval is het aannemelijk dat de rechthebbende zal aanvoeren dat hij een gewichtige reden heeft die gelegen is in het gegeven dat geheimhouding essentieel is voor de werking van het systeem van watermerken en daarmee voor het beschermen van zijn intellectuele eigendom. De rechthebbende heeft in beginsel een rechtmatig belang bij geheimhouding van alle processen die derden kunnen verstoren en de betrouwbaarheid van het watermerk aantasten. Hij zal immers willen voorkomen dat de rapportage ten aanzien van de techniek aanleiding geeft tot gerichte aanvallen op zijn watermerksysteem.

Ten tweede kan erop worden gewezen dat de rechthebbende niet gehouden is aan deze vordering te voldoen wanneer redelijkerwijs aangenomen kan worden dat een behoorlijke rechtsbedeling ook zonder verschaffing van de gevraagde gegevens is gewaarborgd (subsidiariteit). Hiermee worden onder meer de zogenaamde 'fishing expeditions' voorkomen. In de regel zal een beroep op de tweede uitzondering niet snel denkbaar zijn omdat de gedaagde ook een voorlopig deskundigenbericht kan vragen waaraan de rechthebbende in beginsel gehouden is om medewerking te verlenen.[41] Ekelmans merkt onder verwijzing naar zijn eigen dissertatie en die van Sijmonsma op dat deze weigeringsgrond in de praktijk doorgaans weinig betekenis heeft omdat het opvragen van bescheiden efficiënter is dan het aanwenden van een ander bewijsmiddel zoals het getuigenverhoor of deskundigenbericht.[42] Sijmonsma lijkt in zijn dissertatie echter genuanceerder als hij opmerkt dat deskundigenonderzoeken kostbaar en tijdrovend zijn zodat het uit het oogpunt van een goede procesorde in beginsel de voorkeur verdient een deskundigenonderzoek te voorkomen, wanneer het bewijs ook door middel van inzage in bescheiden kan worden geleverd.[43] Ik ben het eens met Sijmonsma dat een deskundigenonderzoek om voorgaande redenen zoveel mogelijk moet worden voorkomen. Dit zal echter niet in alle gevallen mogelijk zijn. Wanneer een partij aangeeft bepaalde vertrouwelijke gegevens nodig te hebben om de betrouwbaarheid van het watermerk te beoordelen zal duidelijk moeten worden of er geen andere wijze is

[37] Het artikel stelt verder als eis dat degene die de exhibitie vordert daarbij een rechtmatig belang heeft, deze exhibitie bepaalde bescheiden of gegevens moet betreffen aangaande een rechtsbetrekking waarin hij of zijn rechtsvoorgangers partij zijn. Voor de verdere uitwerking wordt ervan uitgegaan dat de gedaagde aan deze voorwaarden voldoet. Zie verder o.m. Asser 2013, p. 211. Sijmonsma 2010 (diss.), hoofdstuk 7 en Ekelemans 2010 (diss.) hoofdstuk 6.
[38] Artikel 843a lid 2 Rv.
[39] Artikel 843a lid 4 Rv. Dit lid komt in het huidige Wetsvoorstel 33079 niet in dezelfde bewoording terug. De minister stelt in zijn brief van 21-02-2014 (33079-6) aan de Kamer dat een goede beantwoording van het verslag over het wetsvoorstel tot aanpassing van het inzagerecht alleen mogelijk is wanneer er eerst meer duidelijkheid is over de ontwikkelingen op het terrein van het bewijsrecht.
[40] Zie uitgebreid Sijmonsma 2010 (diss.) hoofdstuk 11, p. 183; Asser 2013, p. 149.
[41] Vgl. Rb. Breda 25 oktober 2006, ECLI:NL:RBBRE:2006:AZ1374, ov. 4.4. waarin de rechtbank in een IE-zaak overweegt dat het bewijs van een onrechtmatige verkoop redelijkerwijs ook langs andere weg kan worden verkregen, waarbij de rechtbank vooral denkt aan het deskundigenbericht.
[42] Ekelmans 2011, p. 349; Ekelmans 2010 (diss.), p. 165-174; Sijmonsma 2010 (diss.), p. 194-198.
[43] Sijmonsma 2010 (diss.), p. 196, voetnoot 34.

waarop de betrouwbaarheid van het watermerk of een onderdeel van het watermerkproces kan worden beoordeeld. In de regel zal dit mogelijk zijn, al zullen daarvoor de nodige tijd en kosten gereserveerd moeten worden. Bijvoorbeeld omdat een deskundige een proefopstelling moet maken. De volgende vraag is of de partij deze gegevens dan zelf in handen mag krijgen en het onderzoek zelf uit mag (laten) voeren of dat deze gegevens in handen moet worden gegeven van een onafhankelijke derde die het onderzoek zal uitvoeren. Er is behoudens de kosten naar mijn mening weinig reden om dit niet door een onafhankelijke derde te laten uitvoeren. Op deze wijze kan immers zowel invulling worden gegeven aan het belang van de waarheidsvinding als aan het belang dat een partij kan hebben om bepaalde informatie vertrouwelijk te houden. De rechter kan daarbij de wijze bepalen, waarop van deze informatie kennis wordt genomen, zodat de gedaagde niet zelf de beschikking krijgt over deze gegevens, maar slechts de beschikking krijgt over de resultaten ten aanzien van de betrouwbaarheid van het watermerk. Het is enkel aan de deskundige om aan te geven welke informatie hij nodig acht.[44] Partijen zijn verplicht hem de gevraagde informatie te verstrekken (art. 198 lid 3 Rv). Uit een weigering tot medewerking kan de rechter de gevolgtrekking maken die hij geraden acht.

Om ervoor te zorgen dat de gedaagde het feit en het bewijsmiddel (watermerk) kan betwisten moet de rechthebbende zijn wederpartij van voldoende aanknopingspunten voorzien.[45] De rechthebbende zal dit in de eerste plaats doen door middel van het deskundigenverslag. Om de rechter te kunnen overtuigen van de betrouwbaarheid van het watermerk als bewijsmiddel zal dit verslag tenminste inzicht geven in de vraag waarom het watermerk als betrouwbaar moet worden aangemerkt.[46] Hiermee is nog niet gezegd dat ook duidelijk is gemaakt waar de risico's liggen ten aanzien van de gebruikte watermerken. In de praktijk van commerciële watermerken zijn de technische en organisatorische elementen veelal geheim, waardoor het zonder medewerking van de rechthebbende voor de gedaagde bijna onmogelijk is om bijvoorbeeld op basis van literatuurstudies zelf meer inzicht te krijgen in de betrouwbaarheid van de gebruikte watermerken.

In beginsel zal het deskundigenverslag veel informatie kunnen bevatten die als aanknopingspunt kan gelden. Zo zal de (partij)deskundige ter onderbouwing van zijn conclusie het watermerkproces op hoofdlijnen beschrijven (toelaatbaarheid) en de gebruikte techniek nader toelichten (betrouwbaarheid). Een risico voor de rechthebbende is dat zijn (partij)deskundige zich voornamelijk zal richten op de aan hem gerichte vraag of het watermerk kan aantonen aan wie het bestand toebehoort.[47] Het is de vraag of er dan in het verslag voldoende

[44] HR 22 februari 2008, ECLI:NL:HR:2008:BB5626, JA 2008/72 m.nt. J. Quakkelaar, ov. 3.6.2.
[45] Het lijdt geen twijfel dat de beschikbare relevante stukken ten aanzien van watermerken voor de wederpartij beschikbaar moeten zijn om bijvoorbeeld een contra-expertise uit te kunnen laten voeren. De gedaagde kan bij een onbereidwillige rechthebbende deze gegevens ook verlangen op grond van art. 22 of 843a Rv. Wanneer rechthebbende weigert de benodigde informatie te verstrekken dan zou de rechter in het nadeel van de rechthebbende moeten oordelen.
[46] Zie par. 6.2 en 6.3.
[47] De uitslag daarvan zal overwegend zijn dat het watermerk naar de licentienemer wijst omdat de rechthebbende in andere gevallen ervoor zal kiezen de rapportage niet bij de stukken te voegen.

aanknopingspunten zijn voor de gedaagde om verweer te kunnen voeren. In de eerste rechtszaken zal het partijen vooraf niet altijd direct duidelijk zijn welke informatie nodig is om 'voldoende' aanknopingspunten te bieden.[48] De rechter zou in de eerste rechtszaken partijen voldoende ruimte moeten bieden hun weg daarin te vinden.

Wanneer de rechthebbende als eiser te weinig aanknopingspunten aan de wederpartij biedt om voldoende verweer te kunnen voeren kan de rechter een aantal keuzes maken. Ten eerste kan de rechter ervoor kiezen om de stelling van de rechthebbende te verwerpen op grond van zijn overtuiging dat deze onvoldoende gemotiveerd gesteld is.[49] Ten tweede kan de rechter ingrijpen in het debat door een aanvullende stel- of mededelingsplicht aan te nemen.[50] Voor nu is het vooral van belang te constateren dat de rechter kan ingrijpen wanneer in dit geval de gedaagde in bewijsnood zou komen doordat de rechthebbende te weinig aanknopingspunten biedt voor het voeren van voldoende verweer ten aanzien van het watermerk. Slaagt de rechthebbende evenwel niet in zijn verzwaarde stelplicht dan zal de uitkomst daarvan het zelfde zijn als wanneer hij niet aan zijn 'gewone' stelplicht zou voldoen, namelijk verwerping van zijn stelling op grond dat deze onvoldoende is betwist. Ten derde kan de rechter er ook voor kiezen om minder hoge eisen te stellen aan de betwisting.[51] In dat geval gaat het proces verder in de wetenschap dat beide partijen ten aanzien van dit feit voldoende hebben gesteld en betwist. De rechter zal dan overgaan naar de fase van bewijslevering en aan de rechthebbende de bewijsopdracht geven (nader) bewijs te leveren voor zijn stelling. Maar zoals gezegd kan de rechter er ook voor kiezen om de stel- of motiveringsplicht van partijen te verzwaren om zo meer zicht te krijgen op de feiten.[52]

De mogelijkheid dat de rechthebbende onvoldoende aanknopingspunten biedt is het grootst in de eerste processen waarin watermerken als juridisch bewijsmiddel worden ingezet. Na verloop van tijd mag van iedere rechthebbende worden verwacht dat hij de rapportage van voldoende aanknopingspunten voorziet.[53] Vanaf dat moment geldt naar mijn mening geen verzwaarde mededelings- of stelplicht meer maar zouden rechters in het geval de

[48] De rechthebbende en serviceverlener zullen pas na een aantal geschillen tot een optimale indeling en inhoud van het verslag (kunnen) komen. Zie voor dat proces ook de wijze waarop rapporteren over DNA in met name het strafrecht tot stand is gekomen en zich nog steeds ontwikkelt (zie par. 6.2).
[49] De sanctie op het niet voldoen aan de motiveringsplicht is immers aan het beleid van de rechter overgelaten.
[50] Bijvoorbeeld naar analogie van de verzwaarde stelplicht (par. 4.3.1.2). Door middel van de informatieplicht kan de rechter ook verhoudingen weer rechtzetten in termen van Equality of arms. Zie Schwartzenberg 2013, p. 93;
[51] Zie ook Van den Brink 2008, p. 93 wanneer hij stelt dat 'een bepaald feitencomplex zich zozeer op het terrein van de wederpartij afspeelt dat aan de concretisering van dergelijke feitelijke stellingen of betwistingen geen al te hoge eisen mogen worden gesteld.
[52] Zie ook Van den Brink 2008, p. 93. De verzwaarde stelplicht of aanvullende stel- of motiveringsplicht wordt in de literatuur veelal beschreven in het kader van een correctie op de bewijslastverdeling (Asser, Rueb), maar wordt ook toegepast in de fase van stellen en betwisten. Het is de rechter op grond van art. 22 overigens altijd toegestaan om partijen te vragen hun stelling aan te vullen of toe te lichten.
[53] Daar komt bij de (partij)deskundige veelal afkomstig zal zijn van de onderneming die de watermerkservice aanbiedt. Deze onderneming zal om die reden dan ook snel ervaring ontwikkelen met het opstellen van rapportages voor juridische procedures.

rechthebbende te weinig aanknopingspunten biedt direct kunnen overgaan tot het oordeel dat de stelling onvoldoende gemotiveerd is gesteld.

De gedaagde die voldoende aanknopingspunten krijgt aangeleverd zal overigens wel voor een ander probleem worden gesteld. Hij zal de aanknopingspunten moeten omzetten naar informatie waarop hij zijn verweer kan baseren. Dat betekent dat hij zelf over kennis moet beschikken en zijn stelling moet onderbouwen op grond van bijvoorbeeld geraadpleegde literatuur of de hulp van een deskundige moet inschakelen om deze informatie om te zetten naar een voldoende gemotiveerd verweer.[54] Bij het voeren van algemene bezwaren, zoals bezwaren ten aanzien van de methodologie, loopt de gedaagde het risico dat deze de rechter niet kunnen overtuigen en dat de hoogste rechter dit oordeel uiteindelijk niet onbegrijpelijk vindt.[55] In de regel zal de gedaagde dan ook de hulp van een deskundige moeten inschakelen om verweer te kunnen voeren tegen de toelaatbaarheid dan wel betrouwbaarheid van het watermerk als juridisch bewijsmiddel.[56] Een deskundige kan hem ten aanzien van de betrouwbaarheid bijvoorbeeld wijzen op gebreken ten aanzien van de inhoud van het verslag of de gebruikte methoden. Hij kan ook zelf onderzoek verrichten en daarover verslag doen. Een belangrijk nadeel daarvan is dat er kosten verbonden zijn aan de inzet van een eigen (partij)deskundige zonder dat vooraf duidelijk is wat de resultaten zijn.

Door de inbreng van het watermerk heeft de rechthebbende zich uiteindelijk een strategisch voordeel verschaft door de gedaagde als het ware te dwingen een deskundige in te schakelen en daarvoor kosten te maken. Weliswaar kan bij een eventuele afwijzing van de vordering van de rechthebbende een volledige proceskostenveroordeling volgen maar dan moet de gedaagde van tevoren weten dat de deskundige een succes voor hem kan boeken.[57] Met de inzet van het watermerk verkrijgt de rechthebbende een goede positie om de gedaagde een schikking te laten overwegen. Zolang de schikking lager is dan de kosten voor een deskundige kan dit in de praktijk snel het overwegen waard zijn.

Wanneer de rechter de stellingen van partijen als voldoende heeft beoordeeld maar het gestelde feit nog niet heeft vastgesteld of heeft verworpen, komen partijen in de fase van het leveren van bewijs. Voordat de rechter partijen, via een tussenvonnis, toelaat tot het leveren

[54] Zie daarvoor ook hoofdstuk zes ten aanzien van het waarderen van watermerken. De daar behandelde psychologische valkuilen zullen evenzeer gelden voor de gedaagde die een verweer probeert te voeren ten aanzien van het watermerk.

[55] Zie voor een vergelijkbare situatie HR 20 november 2009, ECLI:NL:HR:2009:BJ6999 (Lego/Mega Brands) waarin A-G Verkade (ov. 5.12) tot de conclusie komt dat niet is gebleken ‘dat Lego na de confrontatie met het door Mega Brands verrichte marktonderzoek uitdrukkelijk tegenbewijs heeft aangeboden door middel van een eigen onderzoek. Lego heeft ervoor gekozen slechts methodologische bezwaren tegen het rapport aan te voeren, die het hof niet hebben kunnen overtuigen. Het oordeel van het hof acht ik niet onbegrijpelijk.’.

[56] Voor de toelaatbaarheid zal het naast juridische aspecten vooral aankomen op de (technische) vraag of er voldoende technische en organisatorische maatregelen zijn genomen door de rechthebbende.

[57] Uitgangspunt is dan dat het watermerk de doorslaggevende factor zou zijn. In de praktijk is het vanzelfsprekend ook mogelijk dat de rechthebbende op heel andere gronden de zaak verliest.

van bewijs zal hij eerst de bewijslastverdeling en daarmee de bewijsrisicoverdeling van partijen bepalen.[58]

4.2.1.2 Bewijslastverdeling

Op basis van de bewijslastverdeling zal de rechter bepalen welke partij bewijs moet leveren van haar stelling. De regels van de bewijslastverdeling bepalen wie het bewijsrisico loopt, dat wil zeggen welke partij het risico loopt dat de gestelde feiten niet komen vast te staan.[59] Wie het risico draagt hangt niet alleen af van het formele en materiële recht[60] maar ook van de omstandigheden van het geval omdat de rechter de door de wetgever beoogde bewijsrisico-verdeling in de praktijk kan aanpassen en dit ook regelmatig doet.[61] Bijvoorbeeld in de hiervoor kort besproken situatie waarin de verweerder in bewijsnood zou kunnen komen wanneer de rechthebbende onvoldoende aanknopingspunten biedt in zijn rapportage. Voor verdere achtergronden en theoretische onderbouwing van de bewijslastverdeling verwijs ik naar de literatuur.[62]

Bewijslastverdeling volgens de hoofdregel van artikel 150 Rv

Als hoofdregel geldt dat de partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, de bewijslast draagt van die feiten of rechten tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.[63] De stelplicht werkt hiermee door in de verdeling van de bewijslast, namelijk de partij die de stelplicht heeft, draagt in beginsel ook de bewijslast.[64] Aan deze bewijslast is het bewijsrisico verbonden.[65]

---

[58] Partijen zullen ook vooraf deze inschatting maken als onderdeel van het procesrisico.
[59] Bosse 2003 (diss.), p. 15; Asser 2013, p.315; Schwartzenberg 2013, p. 25.
[60] Zo oordeelt de HR 21 februari 1992, NJ 1993, 164 (Cindy/Barbie) in het licht van de effectiviteit van de auteursrechtelijke bescherming dat de ('negatieve') bewijslast rust op de gedaagde dat hij het werk niet heeft ontleend aan het werk van de rechthebbende (in plaats van dat de rechthebbende de ontlening moet stellen en zonodig bewijzen).
[61] Bosse 2003 , p. 15. Bijvoorbeeld omdat de ene partij bewijslevering voor de andere partij bemoeilijkt.
[62] Zie o.m. Asser 2013, p. 304.
[63] Art. 150 Rv. De bewijstlastverdeling is gebaseerd op de zogenoemde objectiefrechtelijke leer die ervan uitgaat dat uit de toepasselijke materiële rechtsregel afgeleid wordt hoe de bewijslast wordt verdeeld en wordt vastgesteld welke elementen nodig zijn om het ingeroepen rechtsgevolg teweeg te brengen. Zie uitgebreid Asser 2013, p. 308; en mede in relatie tot het Belgische recht Bosse 2003 (diss.), p. 20.
[64] Snijders e.a. 2007, nr. 207; De partij die zich op bepaalde rechtsgevolgen beroept draagt de bewijslast van die feiten of rechten. In de regel is dat de eiser, maar de gedaagde die zich beroept op een nieuw feitencomplex en daarmee een zogenoemd zelfstandig of bevrijdend verweer voert zal de nodige feiten moeten bewijzen indien de eisende partij deze betwist. De bewijslast ligt in de dat geval bij de gedaagde.
[65] In dat verband wordt er ook gewezen op de zogenoemde Non liquet, dat ziet op de situatie waarin een of meer van de te bewijzen feiten niet bewezen kunnen worden en de bewijsrisicoverdeling beslissend is. Van den Brink 2008 (p. 95) laat dat mooi zien als hij zegt: 'de partij die zich op een bepaald rechtsgevolg beroept moet de daartoe vereiste feiten stellen (stelplicht) en - als deze betwist worden - bewijzen (bewijslast), en als dat bewijzen niet lukt, treedt dat gewenste rechtsgevolg niet in (bewijsrisico)'. (De verweerder ontkent in dit geval het gestelde feit of recht niet maar beroept zich op een ander feitencomplex. Voor die nieuwe feiten draagt de verweerder dan zelfstandig de bewijslast.)

In het geval een rechthebbende zich op een aangebracht watermerk beroept is er weinig reden om aan te nemen dat de rechthebbende een beroep kan doen op een andere verdeling van de bewijslast. Vanwege een gebrek aan toepasselijkheid van een bijzondere regel uit de wet of jurisprudentie staat hem geen beroep open op grond van een bijzondere (on)geschreven regel. Ook buiten deze bijzondere regel lijkt hem evenmin op grond van de eisen van redelijkheid en billijkheid een andere bewijsverdeling toe te komen.[66] Hoewel de rechter in het geval van bijzondere omstandigheden de bewijslast kan omkeren heeft de Hoge Raad deze gevallen beperkt tot die gevallen waarin de partij die volgens de hoofdregel de bewijslast draagt in een onredelijk zware bewijspositie is gekomen door toedoen van de wederpartij.[67] Daarvan lijkt hier in de regel geen sprake. De Hoge Raad benadrukt de terughoudendheid bij het toepassen van de uitzonderingen en geeft daarmee de voorkeur aan andere methoden om tot verlichting van de bewijslast te komen indien daartoe aanleiding is.[68] Dit kan bijvoorbeeld door de hierna te behandelen vermoedens of een (verzwaarde) motiveringsplicht.[69]

Verlichten van de hoofdregel; vermoedens

Aansluitend op de hoofdregel kan de bewijslast van de rechthebbende nog worden verlicht op grond van zogenaamde vermoedens.[70] In de kern is een vermoeden een bewijsredenering waarbij uit andere feiten het te bewijzen feit wordt afgeleid.[71] Tegen deze vermoedens staat altijd tegenbewijs open. Voor het leveren van tegenbewijs is slechts vereist dat het vermoeden wordt ontzenuwd.[72] Het is niet nodig bewijs van het tegendeel te leveren. Het tegenbewijs is voldoende als het in staat is zodanige twijfel te zaaien dat de op het vermoeden berustende vaststelling onhoudbaar wordt. Een vermoeden levert vooral een voorsprong op omdat het feit bewezen wordt geacht zolang de wederpartij niet slaagt in haar tegenbewijs. Verder gelden de gewone regels van bewijsrisicoverdeling. Anders dan bij de omkering van de bewijslast blijft het risico hier gewoon bij de partij die op grond van de hoofdregel de bewijslast draagt. Dat betekent dat wanneer de feiten uiteindelijk (na enquête en contra-enquête) onduidelijk blijven

[66] Deze regeling biedt de rechter in individuele gevallen de mogelijkheid de bewijslastverdeling te bepalen op grond van overwegingen zoals de processuele houding van partijen, de waarschijnlijkheid dat het feit heeft plaatsgevonden, de vraag welke partij het minst door de bewijslast wordt verzwaard en een positief feit in de regel makkelijker te bewijzen is dan een negatief feit. Zie o.m. HR 22 januari 1993, NJ 1993, 665; Asser 2013, p. 319; Schwartzenberg 2013, p. 34.

[67] HR 7 mei 2004, ECLI:NL:HR:2004:AO2988, NJ 2004, 422 m.nt. DA, ov. 3.4; HR 9 september 2005, NJ 2006, 99; HR 20 januari 2006, NJ 2006, 78, JBPr 2006, 44 m. nt. Rueb, ov. 3.5.5; HR 17 april 2009 ECLI:NL:PHR:2009:BH2955, ov. 3.3; Asser 2013, p. 301, 319; Schwartenberg 2013, p. 86; Van den Brink 2008, p. 97.

[68] Zie naast de hiervoor genoemde arresten ook HR 17 april 2009 ECLI:NL:PHR:2009:BH2955, ov. 3.3.

[69] Eventueel ook door een processueel vermoeden waarbij aan het procesgedrag van een partij een vermoeden wordt ontleend. Zie daarover o.m. Schwartzenberg 2013, p. 108. Zie o.m. Asser 2013, p. 334; Schwartzenberg 2013, p. 77; Asser 2010 in Asser-Nijboer, Schuurmans. nr. 4.5. De partij die verlichting van bewijs wenst zal hiertoe argumenten moeten aandragen waarbij een beroep op de verwezenlijking van de materiële norm een centrale rol zal innemen. Asser 2013, p.; Schwartzenberg 2013, p. 91.

[70] Zie daarover o.m. Asser 2013, p. 326; Schwartzenberg 2013, p. 93.

[71] Zie o.m. Asser 2013, p. 326 Schwartzenverg 2013, p. 99. Zie ook 1953 oud BW: Vermoedens zijn gevolgtrekkingen welke de wet of de rechter uit een bekende tot een onbekende daadzaak afleidt.

[72] HR 2 mei 2003, NJ 2003, 468; Schwartzenberg 2011, p. 197.

de partij die het bewijsrisico draagt verliest.[73] Hoewel het vermoeden ervaren zou kunnen worden als omkering van de bewijslast merkt Snijders op dat een bewijsvermoeden in de praktijk 'gecompenseerd' wordt door een soepele benadering van het tegenbewijs.[74] Dat geldt ook in het geval het tegenbewijs tegen een deskundigenbericht betreft. Dit kan bijvoorbeeld worden geleverd door de inbreng van een eigen expert. Het tegenbewijs moet zich wel richten tegen de vooralsnog aangenomen feiten of omstandigheden.[75]

Ten aanzien van watermerken kunnen vooral het wettelijk en rechterlijk vermoeden een rol spelen bij de waardering van watermerken. Het in de wet opgenomen vermoeden treedt in wanneer de hulpfeiten zijn ingetreden. Bij betwisting daarvan rust de stelplicht bij de partij voor wie het vermoeden werkt. Slaagt hij er niet in deze feiten te bewijzen dan treedt het vermoeden niet in werking.[76]

Voor watermerken bestaat thans geen wettelijk vermoeden. Voor watermerken rijst dan de vraag of aansluiting gezocht kan worden bij het wettelijk vermoeden van de elektronische handtekening (artikel 3:15a BW).[77] In deze regeling worden dezelfde rechtsgevolgen in het leven geroepen voor de elektronische handtekening als voor een handgeschreven handtekening. Dit onder de voorwaarde dat de methode die daarbij gebruikt is voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval.[78] De bedoelde methode wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening (a) op een unieke wijze aan de ondertekenaar is verbonden; (b) het mogelijk maakt de ondertekenaar te identificeren; (c) tot stand komt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en (d) op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden is, dat elke wijziging achteraf van de gegevens kan worden opgespoord; (e) gebaseerd is op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet; en (f) gegenereerd is door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet. Voor watermerken betekent dit dat de methode waarmee de consument zijn gegevens overhandigt (inlogprocedure) aan de bovenstaande eisen zal moeten voldoen. Wanneer aan de bovenstaande eisen wordt voldaan kan de rechthebbende een beroep doen op het wettelijke bewijsvermoeden zoals die geldt voor de elektronische handtekening. Of hiervan sprake is zal per gebruikte methode bepaald moeten worden.[79] In het algemeen is

[73] Schwartzenberg 2013, p. 100.
[74] Snijders in zijn noot onder HR 16 januari 2009, ECLI:NL:HR:2009:BG4012, NJ 2009, 562.
[75] Hof 's-Gravenhage 16 april 2008, ECLI:NL:GHSGR:2008:BM1620, NJ 2010, 204; Wiersma 2010, p. 466.
[76] Zie ook Schwartzenberg 2013, p. 100.
[77] Op 28 augustus 2014 is Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG gepubliceerd in Pub. EU. Deze verordening is per 1 juli 2016 en vervangt dan de richtlijn 1999/93/EG (elektronische handtekening). Zie ook par. 2.2.5.
[78] Zie daarvoor o.m. Voulon 2010 (diss.), p. 251; Van Stekelenburg 2009 (diss.), p. 26. Zie voor de omzetting van de richtlijn 1999/93/EG naar zowel Nederlands als Belgisch recht: o.m. Lodder, Dumortier en Bol 2005.
[79] Zie par. 2.2.5.

het dan ook niet te zeggen of watermerken die als bewijsmiddel worden ingezet gekwalificeerd kunnen worden als een gekwalificeerde elektronische handtekening ex 3:15a BW.

In de regel zal daarvan echter geen sprake zijn omdat dergelijke methoden in de (webwinkel)-praktijk als complex worden ervaren en het gebruiksgemak van consumenten in de weg staat. Rechthebbenden en aanbieders van content lijken hiermee het gebruiksgemak voor consumenten te laten prevaleren boven een meer betrouwbare authenticatiemethode.[80] Wanneer meerdere factoren, zoals de rol die watermerken spelen in het huidige handhavings-beleid (is watermerken het enige handhavingsmiddel of één van de velen), de kosten, het gebruiksgemak voor de consument en het handhavingsbeleid worden afgezet tegen het daadwerkelijk juridische voordeel dat een bewijs vermoeden oplevert, vind ik deze keuze niet onbegrijpelijk.[81] Een bewijsvermoeden levert weliswaar een juridisch voordeel op in die zin dat er sprake is van dwingende bewijskracht, maar er is geen sprake van absoluut bewijs omdat het (terecht) altijd mogelijk blijft om tegenbewijs te leveren. Met name het gevoerde handhavingsbeleid zal bij deze keuze een belangrijke rol spelen. Het handhavingsbeleid van met name de entertainmentindustrie is thans niet gericht op het vervolgen van individuele up- of downloaders waardoor er ook weinig reden is om de huidige authenticatieprocedure erg te verzwaren.[82] Wanneer een rechthebbende echter het watermerk in wil zetten als bewijsmiddel dan zal hij bereid moeten zijn om ook daadwerkelijk tot handhaving over te gaan om te voorkomen dat het watermerk zijn waarde als preventiemiddel niet verliest. Of dat ook betekent dat de rechthebbenden ook over moeten gaan op een authenticatiemethode die voldoet aan de eisen van een gekwalificeerde elektronisch handtekening om daarmee juridisch de meerwaarde van een bewijsvermoeden te krijgen is een zaak die afgewogen moet worden tegen de eerder genoemde factoren, zoals de rol die watermerken spelen in het huidige handhavingsbeleid (is watermerken het enige handhavingsmiddel of één van de velen), de kosten en het gebruiksgemak voor de consument. Het zal ook afhangen van de fase waarin de handhaving zich bevindt. Wanneer consumenten al meer (dan nu) gebruik maken van legaal aanbod zal ook de behoefte aan meer handhaving afnemen.

Nu er geen wettelijk vermoeden in de wet is opgenomen voor watermerken en watermerken in de regel niet als een elektronisch handtekening kunnen worden gekwalificeerd welk een wettelijk bewijsvermoeden oplevert, kan er derhalve geen sprake zijn van een verlichting van de bewijslast.

[80] In de praktijk sluiten rechthebbenden overeenkomsten met diegene die hun content willen aanbieden waarin ook uitgebreide clausules zijn opgenomen over de wijze waarop de aangeboden content ten minste beveiligd moet worden. Vanwege de geheimhoudingsclausules in deze overeenkomsten blijft de exacte inhoud van de overeenkomsten echter geheim.
[81] Het handhavingsbeleid van met name de entertainmentindustrie is thans niet gericht op het aanspreken van individuen die op kleine schaal content up- of downloaden waardoor er ook weinig reden is om de huidige authenticatieprocedure erg te verzwaren (par. 3.3.2).
[82] Zie par. 3.3.2.

Het opstellen van een wettelijk bewijsvermoeden voor watermerken zou de rechthebbende evenals bij alle andere vermoedens een voorsprong opleveren. Er lijkt vooralsnog weinig reden te zijn om een dergelijk vermoeden in de wet op te nemen voor watermerken. Ten eerste moet de wetgever terughoudendheid betrachten bij het formuleren van nieuwe wetgeving. In de eerste plaats lijkt het mij dan ook eerst een kwestie van afwachten hoe dit middel zich in de praktijk ontwikkelt. Naar aanleiding van die ontwikkeling kan de vraag een rol gaan spelen of er behoefte bestaat aan een dergelijk vermoeden. Ten tweede zal erop voorhand weinig maatschappelijk draagvlak zijn voor het instellen van een dergelijk vermoeden. Temeer omdat aan de handhaving van het auteursrecht minder maatschappelijk belang lijkt te worden gehecht dan aan veiligheid en vertrouwen in elektronische communicatie. Dit argument is overigens wel afhankelijk van de toepassing van watermerken. Ten aanzien van watermerken met een authenticatiedoel ten behoeve van bijvoorbeeld paspoorten of rijbewijzen is een Europese richtlijn vergelijkbaar met die van de elektronische handtekening niet ondenkbaar.[83]

Verlichten van de hoofdregel: verzwaarde stelplicht (rechterlijk vermoeden)

Om partijen tegemoet te komen die in bewijsnood verkeren omdat de wederpartij over de relevante gegevens beschikt ten aanzien van het bewijsthema, heeft de Hoge Raad de methode van verzwaarde stelplicht ontwikkeld.[84] Deze methode wordt gehanteerd wanneer de feiten zich ‘in het domein’ hebben afgespeeld van de partij aan wie deze plicht wordt opgelegd en deze partij ook beter in staat is om duidelijk te maken welke feiten zich hebben afgespeeld. In de eerste zaak betrof het een geval uit het merkenrecht waarbij een gedaagde zich beriep op het niet-gebruik (non-usus) van het merk.[85] Daarna heeft de Hoge Raad deze methode ook toegepast in andere zaken, zoals in het medisch aansprakelijkheidsrecht, waarbij de eiser niet deskundig is terwijl de wederpartij over een bijzondere wetenschap bezit. Deze methode is daarna verder toegepast in zaken ten aanzien van het arbeidsrecht en (beroeps-) aansprakelijkheidsrecht.[86]

In de meeste uitspraken van de Hoge Raad betrof het gevallen waarin de partij die de bewijslast draagt niet over aanknopingspunten beschikt om aan haar stelplicht te kunnen voldoen. De (‘deskundige’) partij is er dan toe gehouden om haar betwisting van de haar verweten fout zodanig te motiveren en met de haar ter beschikking staande informatie te

[83] Zie daarvoor ook de overwegingen die aan de richtlijn 1993/93/EG ten grondslag lagen.
[84] Asser 2013, p. 334; Er wordt gesproken over een verzwaarde motiveringsplicht (of verzwaarde of aanvullende stelplicht) die moet worden begrepen in het licht van de bewijsrisicoverdeling. De rechter grijpt in dit geval namelijk in op de bewijsleveringlast door haar te verlichten. Hij grijpt daarmee tevens in op de verdeling van het bewijsrisico van partijen omdat hij de kans dat het risico intreedt verkleint. Zie ook Asser 2013, p. 335; Giesen 2001 (diss.), passim, p. 39; nr. 13, 23 spreekt van een aanvullende stelplicht.
[85] HR 29 november 1957 NJ 1958, 31, NJ 1958/31, BIE 1958, p. 45, AA 1957/58, p. 145 m.nt. DM.
[86] Zie voor het arbeidsrecht o.m. Bosse 2003 (diss.), p. 32 en voor het aansprakelijkheidsrecht o.m. Giesen 2001 (diss.); HR 4 april 2014, ECLI:NL:HR:2014:831, JA 2014/78 m.nt J. Veninga & F.T. Oldenhuis NJ 2014/368 m.nt. T. Hartlief, AB 2014/228 m.nt. A. Hofman; HR 15 juni 2007, ECLI:NL:HR:2007:BA3587, NJ 2007, 335HR 15 december 2006, ECLI:NL:HR:2006:AZ1083, NJ 2007/203, m.nt. Mok (NNE/Mourik);; HR 23 november 2001, NJ 2002, 387; HR 18 februari 1994, NJ 1994, 368.

onderbouwen, dat het de wederpartij aanknopingspunten biedt voor controle en weerlegging, en uiteindelijk voor bewijslevering.[87] Dit brengt uiteindelijk met zich mee dat de verweerder 'gedwongen' wordt zijn stellingen aan te vullen op een wijze die met zich mee kan brengen dat hij bewijs tegen zichzelf aandraagt.[88] De ratio daarachter is dat het gebrek aan een dergelijke mededelingsplicht ertoe zou leiden dat er weinig meer overblijft van de rechtsbescherming die het materiële recht aan deze partij beoogt te bieden.[89]

Voor de rechthebbende is dit leerstuk in zoverre relevant dat het hem duidelijk moet zijn dat de rapportage voldoende aanknopingspunten moet opleveren om verweer te kunnen voeren. Wanneer de rechthebbende dit achterwege laat heeft de rechter verschillende mogelijkheden om het bewijsrechtelijk evenwicht te herstellen. De rechter kan bijvoorbeeld minder zware eisen stellen aan de betwisting door de wederpartij of analoog aan het leerstuk van de verzwaarde stelplicht een verzwaarde motiveringsplicht opleggen aan de rechthebbende. De rechthebbende ontkomt er kort gezegd niet aan om in zijn rapportage voldoende aanknopingspunten te bieden. Het is niettemin aan de wederpartij om haar eigen verweer op te stellen op grond van deze aanknopingspunten, bijvoorbeeld door gebruik te maken van literatuur of een deskundige.

Verlichten van de hoofdregel: voorshands aannemelijk

Een andere wijze waarop de rechter de hoofdregel van artikel 150 Rv kan verlichten is door een feit voorshands aannemelijk te achten.[90] Wanneer een gesteld feit voldoende gemotiveerd is betwist om te voorkomen dat de rechter het feit vaststelt, maar de rechter het wel zeer aannemelijk acht dat het feit zich heeft voorgedaan - bijvoorbeeld in het licht van ander bewijs of op grond van ervaringsregels - kan hij het feit voorshands aannemelijk achten.[91] Op grond van de hoofdregel blijft de bewijslast dan bij de rechthebbende liggen maar hij hoeft, zolang de wederpartij niet slaagt in haar tegenbewijs, (nog) geen bewijs te leveren. Dit vermoeden levert de rechthebbende het voordeel op dat de wederpartij nu de bewijslast draagt, terwijl het bewijsrisico nog steeds bij hem ligt. Met een voorshands oordeel geeft de rechter een voorlopig oordeel dat processueel als consequentie heeft dat de wederpartij (i.c. de licentienemer) de gelegenheid krijgt (tegen)bewijs te leveren. De enquête begint dan anders dan bij een normale bewijslevering met het leveren van tegenbewijs.

[87] Zie Schwartzenberg 2013, p. 93 onder verwijzing naar A-G Huydecoper voor HR 19 november 2004, ECLI:NL:PHR:2004:AR5917, ov. 29; HR 7 september 2001, NJ 2001, 615, ov. 3.4; HR 10 januari 1997, NJ 1999, 286 m.nt. WMK, ov. 3.5.3; HR 18 februari 1994, NJ 1994, 368, ov. 3.3.
[88] Schwartzenberg 2013, p. 92.
[89] Zie Asser 2013, p. 334.
[90] Het voorshands aannemen van een feit wordt naar analogie van het wettelijk vermoeden ook wel een rechterlijk vermoeden genoemd. Hoewel men ook zou kunnen stellen dat een vermoeden vooral op indirect bewijs ziet en een voorhandsaannemelijke bewezenverklaring ook trekken heeft van bewijswaardering. Zie o.m. Van den Brink 2008, p. 96.
[91] Zie o.m. Schwartzenberg 2013, p. 103; Asser 2013, p. 331. Het voorshandsoordeel wordt ook wel omschreven als een rechterlijk of feitelijk vermoeden. Vooral Tjong Tjin Tai 2008, p. 810 en in mindere mate Van den Brink 2008, p. 96 zien de voorshands bewezenverklaring niet als een rechterlijk vermoeden.

Samenvattend ligt ten aanzien van het gestelde feit dat het bestand aan de rechthebbende toebehoort, de bewijslast en het daarbij behorende bewijsrisico op grond van de hoofdregel bij de rechthebbende. Wanneer de rechter het gestelde feit voldoende betwist acht, maar het feit hem wel aannemelijk voorkomt dan kan hij ervoor kiezen een voorshands bewijsoordeel te geven waarin hij een voorlopig bewijsoordeel geeft en de wederpartij toelaat tot tegenbewijs. De fase van bewijslevering begint dan met het leveren van tegenbewijs door de gedaagde (licentienemer). Als de rechter de stellingen van beide partijen voldoende concreet acht maar het feit hem nog niet voorshands aannemelijk voorkomt dan kan hij in een tussenvonnis een bewijsopdracht geven om het nog niet vaststaande feit te bewijzen. In de regel gaat het dan over getuigenbewijs. De rechter kan ook een deskundigenbericht vragen ten aanzien van het watermerk. Na het deskundigenbericht volgen er reacties (contra-enquête e.d.), en geeft de rechter het definitieve bewijsoordeel. De bewijsbeslissing is dan uiteindelijk tot stand gekomen binnen de ruimte die de stellingen van partijen overlaten, en dan soms eerst als voorshands oordeel en dan pas als definitief oordeel.

4.2.1.3 Bewijsaanbod, bewijsopdracht en bewijslevering

Nadat partijen een aanbod tot bewijs hebben gedaan en de rechter dit heeft geaccepteerd kan de rechter in een tussenvonnis een bewijsopdracht geven of een deskundigenbericht vragen.[92] Omdat partijen de schriftelijke stukken veelal eerder in de procedure hebben ingebracht bestaat de bewijsopdracht veelal uit het horen van getuigen en is het leveren van bewijs door middel van schriftelijke stukken eerder uitzondering dan regel.[93]

Een bewijsopdracht wordt pas verleend als iets nog moet worden bewezen en ten aanzien daarvan door partijen een bewijsaanbod is gedaan. Dat betreft zoals gezegd vrijwel altijd getuigenbewijs of deskundigenbewijs. De rechthebbende zal om die reden het watermerk dan ook direct aanvoeren in de stukken en wordt dan ook beoordeeld zonder dat er een specifieke bewijslast door de rechter wordt vastgesteld of een bewijsopdracht is gegeven.

Na het bewijsaanbod kan de rechter beslissen tot het benoemen van een deskundige die hem (en partijen) nader voorlicht ten aanzien van punten waar partijen nog over van mening verschillen of waarvan de rechter een nadere toelichting wenst.[94] Het is aan de rechter om te bepalen of het zinvol is om een deskundigenbericht te gelasten.

Naast het deskundigenbericht kan een partij ook verzoeken om een partijdeskundige te horen (art. 200 Rv). De rechter neemt deze beslissing, die het midden houdt tussen getuigenverhoor en het deskundigenbericht, eveneens in een tussenvonnis.

[92] In de regel zal de rechter een deugdelijk aanbod tot bewijs moeten accepteren.
[93] Asser 2013, p. 179; Schwartzenberg 2013, p. 161.
[94] De rechter wijst de deskundige aan (art. 194 Rv). De rechter is, als er een bewijsaanbod door partijen is gedaan, niet verplicht om een deskundigenbericht te gelasten. HR 6 december 2002, NJ 2003, 63 (Goedèl/Arts); Asser 2013, p. 189; Schwartzenberg 2013, p. 217.

4.2.2 Aannemelijke verweren

Om te voorkomen dat de rechter de stelling van de rechthebbende vaststelt, zal de gedaagde voldoende verweer moeten voeren. De meest aannemelijke verweren zullen zich primair richten op de door rechthebbende te bewijzen stelling dat het op internet aangetroffen bestand aan de licentienemer toebehoort, en de stellingen die de rechthebbende over dat feit en het watermerk heeft aangevoerd.

De gedaagde kan hiertoe drie type verweren voeren. Ten eerste verweren die zich richten op de (juridische) toelaatbaarheid van watermerken als juridisch bewijsmiddel. Bij deze verweren staat de vraag centraal of bij de verkrijging van het watermerk als bewijsmiddel in strijd gehandeld is met het recht en indien dat het geval is of het watermerk van het bewijs moet worden uitgesloten.

Ten tweede verweren die zich richten op de betrouwbaarheid van het watermerk als bewijsmiddel. Bij deze verweren staat de vraag centraal onder welke omstandigheden watermerken de verkeerde uitkomst kunnen geven. De meeste aannemelijke verweren ten aanzien van de betrouwbaarheid van watermerken zijn verweren die zich richten op fouten in het authenticatieproces (verkeerde naam), fouten bij het inzetten van de techniek van watermerken waardoor er sprake kan zijn van een fout-positief, en het verweer dat iemand anders het bestand met ‘zijn’ traitor tracingscode en zonder zijn medeweten heeft verspreid (vals watermerk). Zowel verweren ten aanzien van de toelaatbaarheid als verweren ten aanzien van de betrouwbaarheid raken direct de effectiviteit van het watermerk als juridisch bewijsmiddel. Beide verweren worden verder behandeld in respectievelijk hoofdstuk 5 en 6.

Het derde type verweer dat de gedaagde kan voeren zijn verweren ten aanzien van het gestelde feit. Deze verweren richten zich op de conclusie die de rechthebbende wil verbinden aan het feit dat het op internet aangetroffen bestand aan de gedaagde toebehoort. Bij dit type verweer betwist de gedaagde niet dat het bestand aan hem toebehoort, maar richt hij zich op alternatieve verklaringen die het gestelde feit verklaren. Dit laatste verweer zal hierna verder worden uitgewerkt. Dit verweer zal zich dan voornamelijk richten op de stelling dat iemand anders het bestand op internet heeft gezet, bijvoorbeeld omdat zijn computer is gehackt of dat anderen ook toegang hadden tot dit bestand. Voor de effectiviteit van het watermerk als juridisch bewijsmiddel is dit verweer verder niet meer van belang, omdat dit type verweer het gestelde feit als uitgangspunt neemt. Niettemin kan het wel een belangrijke rol spelen bij het vaststellen van de feiten die nodig zijn om inbreuk op het auteursrecht te kunnen vaststellen.[95] In het bijzonder bij het leggen van een verband tussen het op internet aangetroffen bestand en het feit dat de licentienemer degene is geweest die het bestand geopenbaard heeft.[96] Dit type

[95] Jurisprudentie-onderzoek op de termen [auteursrecht, uploaden] levert op 30 december 2014 op rechtspraak.nl 30 resultaten op. In deze zaken betreft het voornamelijk het faciliteren van inbreuk door het bieden van gelegenheid, veelal via technieken die tegelijk up-en-downloaden faciliteren. Het uploaden van de bestanden wordt door de rechter vaak vastgesteld op grond van de gebruikte techniek (techniek verplicht je bij downloaden ook tot uploaden).

[96] In de regel zal het in zaken waarbij het bekende werken betreft die op internet zijn aangetroffen aankomen op de vraag of bewezen kan worden wie de bestanden op internet heeft geplaatst dan wel deze verder heeft

verweer is voor de gedaagde in beginsel aantrekkelijk om te voeren. Dit verweer kan immers altijd en dus ook los van de toelaatbaarheid en betrouwbaarheid van het watermerk worden gevoerd.

In de praktijk lijken alternatieve verklaringen echter niet eenvoudig in te roepen.[97] Ten eerste moet de verklaring passen binnen de reeds bekende feiten om te voorkomen dat de eiser ze eenvoudig kan pareren en het verweer niet het benodigde vertrouwen wekt.[98] Ten tweede zal de gedaagde die een dergelijk verweer wil voeren dit verweer moeten motiveren. Het enkel wijzen op de mogelijkheid dat er bijvoorbeeld een hack heeft plaatsgevonden is niet voldoende. Dit te meer omdat deze feiten meer in het domein van de gedaagde dan van de rechthebbende liggen. De blote stelling dat 'iemand anders' het bestand op internet heeft gezet zal zonder nadere onderbouwing dan ook niet slagen. Welke verklaringen mogelijk zijn hangt mede af van de andere omstandigheden van het geval. Indien bijvoorbeeld in de procedure al duidelijk is geworden dat de bestanden van de computer (IP-adres) van gedaagde zijn verstuurd dan zullen verklaringen die daarmee niet stroken weinig zin hebben.[99] De stelling dat 'iemand anders' het bestand op internet heeft gezet zal de gedaagde altijd moeten onderbouwen met veelal nieuwe feiten. Primair zal het gaan om de stelling dat een ander toegang had tot de computer waar zijn bestanden op stonden opgeslagen.[100] De gedaagde kan deze toegang zelf vrijwillig hebben geboden door bijvoorbeeld zijn wachtwoord te delen, maar iemand anders kan ook tegen de wil van de gedaagde toegang tot zijn computer hebben verkregen bijvoorbeeld als zijn computer is gehackt.

In beide gevallen zal de rechthebbende er uiteindelijk voor kiezen om de stelling te betrekken dat op de licentienemer een zorgplicht rust om de computer toereikend te beveiligen of anders de gevolgen in termen van aansprakelijkheid ervan te dragen. Voor beide situaties geldt dat er ook bij het gebruik van ICT een trend zichtbaar is dat er ook in deze gevallen een zorgplicht geldt voor gedaagde.[101]

---

verspreid. Uit het enkele gebruik van een IP-adres dat toebehoort aan Sanoma kan niet worden opgemaakt dat er sprake zou zijn van bewust uitlekken door Sanoma, als marketingstrategie; Rb. Amsterdam 12 september 2012 ECLI:NL:RBAMS:2012:BX7043, ov. 4.13 (Sanoma & Playboy/GS Media; Brit).

[97] Jurisprudentie-onderzoek op de termen [auteursrecht, uploaden] leverde op 30 december 2014 op rechtspraak.nl 30 resultaten op waarin geen relevant alternatief verweer is gevoerd. In het strafrecht hebben Koops & Stevens 2010 het gebruik van alternatieve verweren onderzocht in het kader van kinderporno (par. 4.4.2).

[98] Zie bijvoorbeeld HR 8 juli 1992, NJ 1992, 713. Zo stelt de Rb. Roermond 23 december 2009 ECLI:NL:RBROE:2009:BK7698 (ov. 7) in een strafzaak (maar de overweging is in het civiele recht evenzeer mogelijk) geen geloof in een verklaring van verdachte omdat '[verdachte] telkens zijn verklaringen wijzigt dan wel met nieuwe verklaringen komt, waarbij opvalt dat zulks telkens gebeurt nadat er weer wat meer of andere, voor hem belastende, informatie aan [verdachte] bekend wordt (gemaakt)en laat hij na zijn verklaringen te onderbouwen.'

[99] Zie voor het gebruik van een IP-adres als bewijs o.m. Rb. Amsterdam 12 september 2012. ECLI:NL:RBAMS:2012:BX7043, ov. 4.13 (Brit); Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (Ziggo/123 Video). Met name in het strafrecht zijn vanwege de uitgebreide motivering aanwijzingen te vinden die ook de civiele rechter kunnen helpen bij het komen tot zijn oordeel.

[100] Hierbij moet niet alleen aan computers worden gedacht maar ook aan bijvoorbeeld toegang tot Cloud-diensten met behulp waarvan content is opgeslagen.

[101] Zie ook Van der Hof in haar noot onder Rb. Rotterdam 20 april 2011, ECLI:NL:RBROT:2011:BQ7167, CR 2011/159 (BizKey) die constateert dat 'toerekening van het risico voor onzorgvuldig gebruik van de

Zo oordeelde de rechtbank Zutphen in een geschil tussen een bank en vennoten van een VOF dat voor de beantwoording van de vraag wie van de partijen het risico draagt dat misbruik is gemaakt van de elektronische handtekening, relevant is aan wie valt toe te rekenen dat een onbevoegde persoon de beschikking heeft gekregen over zowel de Biz Key als de bijbehorende inlogcodes (deze vormen samen de elektronische handtekening). De rechtbank oordeelde dat in beginsel wordt aangenomen dat het misbruik te wijten is aan een gebrek aan zorg van in dit geval de klant.[102] Dit zal volgens de rechtbank slechts anders zijn onder door de klant te stellen en te bewijzen omstandigheden die een zodanig gebrek aan zorg uitsluiten.[103] Dit zal niet anders zijn wanneer het enkel om inlogcodes gaat, bijvoorbeeld bij een onlinewinkel of creditcard.[104] Ook kan een zorgplicht worden aangenomen in situaties waarin de stelling wordt betrokken dat de drager is gestolen en dat de dief of iemand anders vervolgens de bestanden heeft verspreid.[105] Deze zorgplicht kan, afhankelijk van de omstandigheden van het geval, worden aangenomen voor alle verweren die er in de kern op neerkomen dat iemand anders toegang heeft verkregen tot zijn computer. De zorgplicht is vanzelfsprekend niet zaligmakend voor de rechthebbende. Immers wanneer de licentienemer kan aantonen dat hij aan deze zorgplicht heeft voldaan neemt de kans af dat zijn vordering door de rechter wordt toegekend. En mogelijk is dat in de meeste gevallen ook terecht en kan het voldoen aan alle zorgplichten erop wijzen dat de licentienemer het daadwerkelijk niet heeft gedaan dan wel voldoende maatregelen heeft genomen om te voorkomen dat het bestand op internet is geplaatst. Het is uiteindelijk een vraag naar de risicoverdeling tussen partijen. Daar kan verschillend over worden gedacht. In zaken waarin een consument voldoende zorg heeft betracht om ongeoorloofde verspreiding te voorkomen lijkt er mij weinig reden om af te wijken van een regeling waarin door middel van de zorgplicht tot een risicoverdeling wordt gekomen. Wanneer een consument voldoet aan deze zorgplicht zal dat tot gevolg hebben dat hij niet aansprakelijk kan worden gehouden voor het openbaar maken van het werk.

De rechthebbende kan de zorgplicht, in navolging van banken, nader regelen in de (licentie)-overeenkomst. Zo wordt in de algemene (betalings-)voorwaarden van de ABNAmro bank onder meer gesteld dat klanten alleen gebruik mogen maken van ‘geschikte, veilige apparatuur en programmatuur met toepassing van de meest actuele veiligheidsmaatregelen, antivirusprogrammatuur en firewall(s), tegen virussen, spyware, phishing en ander

elektronische handtekening een vraagstuk (is) dat in de moderne samenleving, waarin het contractuele en meer algemeen communicatieverkeer vaker digitaal plaatsvindt, steeds meer zal voorkomen.’ Zie ook TjongTjin Tai & Koops 2015 en het rapport waarop zij dit artikel baseren.

[102] De Nederlandse Vereniging van Banken (NVB) presenteerde eind 2013 vijf uniforme veiligheidsregels (veiligbankieren.nl) waaruit kort gezegd een zorgplicht blijkt voor consumenten om er zeker van te zijn dat de bank fraude met internetbankieren vergoedt. Deze regels zien o.m. op het vertrouwelijk houden van pincodes en wachtwoorden en de plicht om de computer te voorzien van actuele beveiligingssoftware.

[103] Rb. Zutphen 22 februari 2012 ECLI:NL:RBZUT:2012:BX1620, ov. 5.3.

[104] Zie daarvoor HR 19 november 1993, NJ 1994, 622, m.nt. JCS (COVA); Rb ‘s-hertogenbosch 24 februari 2011, ECLI:NL:RBSHE:2011:BP5939. Het aansprakelijkheidsrecht wordt hier verder buiten beschouwing gelaten. Zie over een nadere uiteenzetting van het aansprakelijkheidsrecht bij vervalste handtekeningen o.m. Emes 2011.

[105] Eén van de factoren kan zijn dat de licentienemer bij diefstal wel aangifte moet doen. Een dergelijke voorwaarde kan ook in de licentieovereenkomst worden opgenomen.

misbruik'.[106] Naast bewijsrechtelijke beperkingen in het consumentenrecht is het in de praktijk ook de vraag in hoeverre klanten bereid zijn tot aanvaarding van deze voorwaarden. Enerzijds verschaft het de gebruiker toegang tot unieke content waarvoor hij mogelijk bereid is de voorwaarden te accepteren. Anderzijds is het niet ondenkbaar dat afnemers, evenals bij de kopieerbeveiliging, beperkende (juridische) voorwaarden niet accepteren voor deze groep (entertainment-)producten. Met als gevolg dat zij niet langer de bereidheid hebben om deze producten te kopen.

Samenvattend zijn verweren die zien op de toelaatbaarheid en betrouwbaarheid de twee meest aannemelijke verweren die de gedaagde zal voeren ten aanzien van het watermerk als juridisch bewijsmiddel. Daarnaast kan de gedaagde nog alternatieve verklaringen aanvoeren waarin hij kort gezegd niet het gestelde feit betwist maar stelt dat het bestand door een ander op internet moet zijn geplaatst. Dit type verweer raakt de effectiviteit van het watermerk niet. Het verweer raakt immers het gestelde feit niet, maar richt zich op het verband tussen de licentienemer en de openbaarmaking van het bestand. Zonder dit verband is kort gezegd de licentienemer niet aan te wijzen als inbreukmaker. Dit type verweer is in de praktijk echter niet eenvoudig te voeren omdat de verklaring die de licentienemer stelt binnen het feitencomplex van de zaak moet passen. Bovendien zal hij niet kunnen volstaan met een blote stelling, maar zal hij zijn stelling dat 'een ander het heeft gedaan' moeten motiveren en onderbouwen. Niettemin is het een verweer dat mogelijk blijft. Niet in de laatste plaats omdat het mogelijk is dat de licentienemer het bestand daadwerkelijk niet op internet heeft geplaatst, noch voor de plaatsing daarvan enige verantwoordelijkheid draagt in het licht van de zorgplicht.

4.2.3 Beslissen over feiten: het bewijsoordeel

Het is uiteindelijk aan de rechter overgelaten om in het licht van de stellingen van partijen het bewijs te waarderen en een oordeel te vormen over het gestelde feit. Pas wanneer de gedaagde betwist dat het bestand naar hem wijst wordt de rechterlijke overtuiging ten aanzien van het watermerk van belang. Alleen dat bewijs hangt immers geheel van het watermerk af.

Om tot een beslissing te kunnen komen zal de rechter moeten nagaan of hij vrij is in de waardering van het watermerk of dat er beperkingen zijn gesteld aan de waardering daarvan (par. 4.2.3.1). De Bock introduceerde in haar proefschrift een nieuw bewijswaarderings-criterium. Aan de hand van de beoordeling van het watermerk zal worden onderzocht hoe dit criterium in de praktijk zal werken (par. 4.2.3.2). Tot slot is er aandacht voor de vraag welke rol de deskundige kan spelen bij het waarderen van het watermerk (par. 4.2.3.3).

[106] Zie artikel 13 Algemene voorwaarden van februari 2010 en meer specifiek art. 17-19 Algemene Voorwaarden Toegang ABN AMRO van januari 2007 (website ABN AMRO 30 december 2014). Zie ook http://kassa.vara.nl/tv/afspeelpagina/fragment/slachtoffer-van-malware-bij-abn-amro-geen-compensatie/speel/1/.

4.2.3.1 Beslissen over watermerken

Voor het waarderen van bewijs geldt in Nederland de vrije bewijsleer, waarbij als hoofdregel geldt dat de rechter vrij is in de waardering van het bewijs (art. 152 Rv). Dat betekent dat het in beginsel aan de rechter is om te bepalen of hij overtuigd is dat het watermerk bewijs levert van het gestelde feit.[107]

De wetgever heeft de rechter echter niet in alle gevallen vrijgelaten in de waardering van het bewijs. Belangrijke uitzonderingen ten aanzien van het watermerk als bewijsmiddel kunnen worden gevonden in dwingend bewijs en in de bewijsovereenkomst.[108]

Ten aanzien van bewijsmiddelen spreekt de wet ook wel van dwingend bewijs of bewijsmiddelen met dwingende bewijskracht.[109] Dwingend bewijs houdt in dat de rechter verplicht is de inhoud van bepaalde bewijsmiddelen als waar aan te nemen of verplicht is de bewijskracht te erkennen die de wet aan bepaalde gegevens verbindt. Het dwingende karakter hiervan is overigens beperkt omdat tegenbewijs mogelijk is, tenzij de wet het uitsluit.[110] Anders dan voor de elektronische handtekening geldt voor het gebruik van watermerken geen wettelijk vermoeden waardoor er ook geen sprake is van dwingende bewijskracht ten aanzien van het gebruik van watermerken in het licht van het gestelde feit. De rechter blijft derhalve vrij in de waardering van watermerken.

Partijen kunnen, voor zover het bewijs van deze feiten ter vrije bepaling van partijen staat, ook zelf de waarderingsvrijheid van de rechter beperken door bij het aangaan van in dit geval de licentieovereenkomst bepalingen op te nemen waarin zij de feitenvaststelling en het bewijsrisico vooraf regelen (art. 153 Rv).[111] De wetgever heeft partijen wel beperkt door wettelijke gronden op te nemen waarop deze overeenkomsten buiten toepassing kunnen worden verklaard.[112] Ten aanzien van watermerken is het vooral van belang dat de rechthebbende niet mag afwijken van dwingende wetsbepalingen ten aanzien van consumenten. Zo mogen geen bepalingen worden opgenomen die deze groep uitsluiten of

[107] Zie naar Nederlands civiel recht o.m. Asser 2013, p. 273; Schwartzenberg 2013, p. 191; Van Stekelenburg 2009 (diss.), p. 52; HR 5 december 2003, NJ 2004, 74; zie naar Belgische civiel recht o.m. Allermeersch 2007 (diss.), p. 463; zie voor het Belgische strafrecht o.m. Verstraeten 2012.

[108] Verder kan er nog op worden gewezen dat de rechter niet toekomt aan de waardering van het bewijs wanneer het bewijs uitgesloten dient te worden. Daarnaast heeft de wetgever soms het soort bewijsmiddelen beperkt waarmee bewijs kan worden geleverd en soms wordt de rechter geïnstrueerd om geen al te hoge eisen aan het bewijs te stellen. Zie o.m. Asser 2013, p. 286.

[109] Art. 151 lid 1 Rv. Eventueel beperkt bewijs zal in het kader van dit onderzoek niet nader worden besproken

[110] Art. 152 lid 2 Rv; Met dwingend bewijs wordt volgens Asser (2012, p. 285) kennelijk gedoeld op wettelijke vermoedens waartegen zoals bij alle vermoedens ook altijd tegenbewijs is toegelaten. Zie ook Hidma & Rugters 2004, p. 32.

[111] Zie o.m. naar Nederland civiel recht Asser 2013, p. 110; Schwartenzenberg 2013, Van Stekelenburg 2009 (diss.), p. 52; Hidma & Rutgers 2004, p. 71. Parl. Gesch. Nieuw bewijsrecht, p. 98. Tegenbewijs is in beginsel mogelijk, maar de rechter is daartoe volgens vaste jurisprudentie niet ambtshalve verplicht. HR 19 december 1949, NJ 1950, 51.

[112] Art. 153 Rv. Denk hierbij aan nietigheid op grond van 3:40 BW, de derogerende werking van de redelijkheid en billijkheid (6:248 BW) of nietigheid of vernietigbaarheid wegens strijdigheid met een dwingende bepaling. Asser 2013, p. 112.

beperken om bewijs te leveren of de bewijslastverdeling ten nadele van de consument wijzigen.[113] Dat brengt met zich mee dat de rechthebbende in beginsel op bepalende onderdelen nauwelijks van het wettelijk bewijsrecht kan en zal afwijken.[114]

De rechter zal in de regel dan ook vrij zijn in de waardering van het watermerk. Ook de vooral schriftelijke vorm waarin het watermerk zal worden gepresenteerd maakt dit niet anders. Voor de bewijskracht van geschriften heeft de wetgever een onderscheid gemaakt tussen akten en geschriften die geen akten zijn.[115] De rapportage behoort tot deze laatste categorie en daarvoor geldt een vrije bewijskracht. Dit geldt ook voor rapporten die op verzoek van de rechter door deskundigen worden ingebracht.[116] De waardering van en de mate waarin het watermerk overtuigt, ligt geheel bij de rechter.

De rechter ziet zich dan geconfronteerd met de vraag hoe hij het watermerk moet waarderen. Voor digitale watermerken bestaat erop dit moment geen aparte wetgeving waarin de waardering ervan nader is vastgelegd.[117] Voor het waarderen van watermerken zou de vraag kunnen rijzen of aansluiting gezocht moet worden bij de criteria die zijn genoemd voor het intreden van het wettelijk vermoeden van de elektronische handtekening (artikel 3:15a BW).[118] Daar lijkt echter geen aanleiding toe nu de functionele beschrijving van de elektronische handtekening reeds verschilt van die van watermerken. Daarnaast houdt de rechter ook daar nog redelijk veel ruimte om zelf te beoordelen of hij de methode betrouwbaar acht.[119]

---

[113] Zie daarvoor verder als aangegeven in artikel 6:236 onder k BW. Deze bepalingen zijn onredelijk bezwarend en vernietigbaar op grond van 6:233 BW.

[114] Zo heeft bijvoorbeeld ook bol.com [30-12-2014] geen afwijkende bepalingen opgenomen in haar algemene voorwaarden en worden er ook geen andere algemene voorwaarden gesteld bij de aanschaf van e-books met watermerken.

[115] art. 156, lid 1 Rv.

[116] art. 194 Rv.

[117] Zo meldt de Regeling van de Minister van OCW van 15 maart 2012, nr. BVE/Stelsel/294391, houdende vaststelling van modellen en technische veiligheidseisen voor diploma's en resultatenlijsten mbo (Regeling modeldiploma mbo) in artikel vijf slechts dat het waardepapier een uniek watermerk moet bevatten maar niet op welke wijze dat moet worden aangebracht en zelfs niet of deze analoog of digitaal, en waarneembaar of onwaarneembaar moet zijn. Zie ook de bijlage bij Regeling van de Staatssecretaris van OCW van 10 juni 2008, nr. VO/OK/2008/51284, houdende modellen diploma's, cijferlijsten, certificaten, getuigschrift, bewijs van ontheffing met verklaring v.w.o.-h.a.v.o.-v.m.b.o. en getuigschrift praktijkonderwijs (Regeling modellen diploma's v.w.o.-h.a.v.o.-v.m.b.o.). Zie ook reglement camera's op de ambulance (Protocol UMCG) uitgegeven 5 oktober 2009 (richtlijn 26-04-2010), p. 2 waarin een watermerk aan beelden wordt toegevoegd om de echtheid van de opnames te garanderen. In Europees verband is dit niet anders: zie Richtlijn 2007/46/EG van het Europees Parlement en de Raad van 5 september 2007 tot vaststelling van een kader voor de goedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd (Kaderrichtlijn) waarin het watermerk wordt gebruikt om vervalsing tegen te gaan (art. 18 lid 3).

[118] Zie daarvoor o.m. Voulon 2010 (diss.), p. 251; Van Stekelenburg 2009 (diss.), p. 26. Zie voor de omzetting van de richtlijn 1999/93/EG naar zowel Nederlands als Belgisch recht: o.m. Lodder, Dumortier & Bol 2005. Zie verder het Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (4.6.2012, COM(2012) 238.

[119] Zie uitgebreid Van Stekelenburg 2009 (diss.), p. 79.

Er lijkt ook weinig reden om wetgeving ten aanzien van de waardering van watermerken te maken. Naast de vraag naar de maatschappelijke wenselijkheid van een dergelijke bepaling dient ook de vraag te worden gesteld of wetgeving ook daadwerkelijk bij zou dragen aan een betere waardering van het watermerk en daarmee aan de (juridische) waarheidsvinding. Op wetgevingsniveau is de beoordeling van elektronische gegevens vaak slechts functioneel beschreven om ruimte te bieden aan nieuwe ontwikkelingen.[120] Daar hoort dan echter ook bij dat de rechter de ruimte moet hebben om die ontwikkelingen een plaats te geven. Dat kan in de loop van de tijd door eigen kennis maar zal vooral plaatsvinden met behulp van deskundigen. Zonder nadere wetgeving is de rechter aangewezen op criteria die zijn opgesteld in vergelijkbare gevallen in de wetgeving, jurisprudentie of de kennis van deskundigen.

In Nederland zijn, evenals in Verenigde Staten, België, Duitsland, Frankrijk en het Verenigd Koninkrijk, vooralsnog geen rechtszaken gevoerd waarin onzichtbare digitale watermerken als bewijsmiddel werden ingezet en de betrouwbaarheid daarvan ter sprake kwam.[121]

Van Stekelenburg constateert dat in de Nederlandse jurisprudentie niet duidelijk wordt welke criteria de rechter gebruikt bij de waardering van elektronische gegevens. Hij noemt hiervoor in navolging van Kemna twee redenen.[122] Ten eerste noemt hij de beperkte motiveringsplicht die de rechter niet verplicht tot nadere motivering en ook niet door de rechter zelf verder wordt ingevuld. Ten tweede noemt hij de processuele rol die er volgens hem toe kan leiden dat deze gegevens niet worden ingebracht als bewijs, onvoldoende worden betwist, de rechter een impliciete beoordeling maakt van de bewijsmiddelen, zijn oordeel reeds op ander bewijs heeft gebaseerd of onvoldoende bekend is met manipulatiemogelijkheden van ogenschijnlijk ingebrachte elektronische middelen.[123] Daarnaast wijzen Kemna en Van Koppen dan ook terecht beiden op de risico's van het leveren van bewijs. Kemna legt ten aanzien van elektronisch bewijs de nadruk op het gebrek aan zekerheid nu de rechter bij het gebrek aan normen geheel vrij is in de waardering en het dus maar afwachten is hoe de beslissing uitpakt.

---

[120] Van Stekelenburg 2009 (diss.), p. 190, 193. In zijn onderzoek richt hij zich met name op e-mail als bewijsmiddel.

[121] In eerdere zaken in de Verenigde Staten speelden watermerken wel een rol maar kwam de betrouwbaarheid daarvan niet ter sprake (zie o.m. US Court of Appeals, 14 februari 2005, 398 F.3d 1193, 10th Cir., 2005 inzake Palladium Music, Inc./ EatSleepMusic, Inc.; US District Court, 18 november 2004, 346 F. Supp. 2d 1068 inzake Warner Bros./Carmine Caridi et al.). Zie ook HvJ EU 30 september 2010, zaak C-581/08, ECLI:EU:C:2010:559, NTFR 2010, 2319 m.nt. Sanders (EMI Group), ov. 10 (voetnoot 3, hfst 1). In de zaak Bruno Press/Image Media (Vzr. Rb. Amsterdam 16 oktober 2008, Mf 2008-11/12, 39, m.nt. Alberdingk Thijm) werden zichtbare digitale watermerken ingezet en werd de techniek verder niet betwist. In de zaak, vzr. Rechtbank Arnhem, 22 mei 2008, ECLI:NL:RBARN:2008:BD3441 (De Roode Roos) vormde het watermerk niet alleen een bewijsmiddel maar maakte het ook onderdeel uit van het werk. In deze zaak achtte de rechtbank het watermerk (Roode Roos) het enige oorspronkelijk element en door dit achterwege te laten waren de productfoto's verder niet origineel en was er derhalve geen sprake van inbreuk op het auteursrecht (ov. 4.5). In de zaak tussen NUV en Tom Kabinet inzake het aanbieden van tweedehands e-boeken kwam het digitale watermerk als bewijsmiddel wel ter sprake maar is deze als bewijmiddel niet beoordeeld (vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet), ov. 2.4; in hoger beroep speelt het watermerk helemaal geen rol meer (Hof Amsterdam, 20 januari 2015 ECLI:NL:GHAMS:2015:66).

[122] Kemna 2004, p. 214. Van Stekelenburg 2009 (diss.), p. 58, 193.

[123] In de Verenigde Staten worden overeenstkomstige argumenten genoemd. Zie Kessler 2010 (diss.), p.8 en de daar aangehaalde literatuur.

Van Koppen wijst ten aanzien van technisch bewijs op de risico's in de bewijsketen waardoor het veel makkelijker is een gat te schieten in de bewijsvoering en de keuze eerder zal vallen op de inzet van een verklaring als bewijsmiddel dan forensisch technisch bewijs.[124]

Van Stekelenburg vindt het opmerkelijk dat 'de authenticiteit van objecten of gegevens weinig aandacht krijgt in de [civiele] rechtspraak, juist omdat deze ook vaak zo eenvoudig te vervalsen zijn'. Hij geeft daarbij als verklaring dat 'als partijen niet noemen dat de gegevens weleens gemodificeerd zouden kunnen zijn, de rechter zich hier ook niet op richt'.[125] Ik deel zijn observaties dat erop basis van de gepubliceerde jurisprudentie weinig aandacht lijkt te zijn voor de betrouwbaarheid van digitaal bewijs en dat partijen daarvoor meer aandacht kunnen vragen.[126] Op basis van de gepubliceerde jurisprudentie kan men zich tegelijk ook afvragen in hoeverre de modificatie van gegevens in de (rechts)praktijk voorkomt en daadwerkelijk een probleem vormt. Vanzelfsprekend kan een gebrek aan aandacht hiervoor in het kader van de waarheidsvinding een probleem vormen, wanneer aangetoond zou kunnen worden dat er vaak sprake is van gemodificeerd bewijs. Onderzoek hiernaar is mij echter onbekend. Daarnaast zal gemodificeerde bewijs in de rechtspraktijk niet in alle gevallen een probleem vormen. Het is immers ook heel goed mogelijk dat de betrouwbaarheid van de gegevens niet van doorslaggevende betekenis is. Bijvoorbeeld omdat er meer bewijs voorhanden is waarop het eindoordeel gebaseerd kan worden en het gemodificeerde bewijs geen doorslaggevende rol speelt. Tegen die achtergrond is het dan de vraag hoe vaak het uiteindelijk voorkomt dat gemodificeerd bewijs een doorslaggevende rol speelt bij het komen tot een eindoordeel. Niettemin geldt ook hier dat iedere zaak waarin dat wel het geval is, er één te veel is.

Die conclusie vormt de brug naar het tweede deel van de observatie, namelijk dat partijen er meer aandacht voor zouden kunnen vragen. In de praktijk zullen vooral kosten en de mogelijkheden om een dergelijk onderzoek te verrichten een grote rol spelen. Bij de kosten moet vooral worden gedacht aan het inhuren van voldoende forensische expertise om het onderzoek te kunnen verrichten. Dat onderzoek zal echter niet (meer) in alle gevallen mogelijk zijn.[127] Het zal duidelijk zijn dat wanneer het bewijs, waarmee je wilt bewijzen dat aangebracht bewijs gemodificeerd is, op bijvoorbeeld één van de 690 servers stond het nagenoeg onmogelijk is modificatie van bewijs te bewijzen. De vraag die dan gesteld kan worden is of dit verschilt van fysiek bewijs, zoals een overeenkomst op papier. Het antwoord

[124] Van Koppen 2011, p. 121.
[125] Van Stekelenburg 2009 (diss.), p. 210.
[126] Onderzoek in het strafrecht wijst ook uit dat in het kader van de waarheidsvinding een actieve bijdragen van partijen gewenst is (par. 4.4.3.2).
[127] Zo wiste het Nederlandse hostingbedrijf Leaseweb de 690 servers met daarop de data van gebruikers van Megaupload (http://webwereld.nl/datacenter/78217-leaseweb-wist-megaupload-data-van-630-servers (laatst geraadpleegd 31-12-2013)). De belangen om servers 'beschikbaar' te houden zijn zo groot, zo stelde het hostingbedrijf Carpathia, dat het bewaren van de Megaupload-data 9000 dollar per dag kostte. Het achterhalen van gegevens is vooral een kwestie van het afwegen van belangen en kosten. In veel gevallen is het technisch nog wel mogelijk de data terug te halen, maar moet daarbij ook rekening worden gehouden met kosten die samenvallen met bijvoorbeeld het stilleggen van servers of in dit geval de belangen van de nieuwe huurder.

is lastig te formuleren bij gebrek aan vergelijkend onderzoek. Maar op het eerste gezicht lijkt het in een digitale omgeving eenvoudiger om bewijs en sporen te maken. Het lijkt met andere woorden eenvoudiger om een totaalplaatje (bewijs en context) te manipuleren. Eenmaal in de mailserver kun je meerdere emails plaatsen, versturen, etc. Dat lijkt mij op het eerste gezicht lastiger bij fysiek bewijs. Daar staat tegenover dat het waarschijnlijk ook eenvoudiger (maar wel kostbaar) is om daarvan sporen te vinden. Maar ook daar geldt 'the absence of evidence is not the evidence of absence'. Dat betekent dat het ontbreken van bijvoorbeeld sporen van een hack, niet betekent dat er geen hack heeft plaatsgevonden. Om dat te kunnen bepalen is vaak meer informatie nodig. De hulp van een expert is daarbij noodzakelijk. Alleen hij kan de rechter een beter beeld geven. Uiteindelijk gaat het dan om de vraag wie de bewijslast draagt en of hetgeen bewezen moet worden kan worden bewezen. Daarbij gaat het niet alleen om digitaal bewijs maar ook en misschien wel vooral om ander bewijs dat bijdraagt aan de totale puzzel. Dat geldt ook voor het opsporen van een hack. Enerzijds bestaat het opsporen uit het zoeken van technische sporen en anderzijds uit het zoeken naar ander bewijs dat de hack heeft plaatsgevonden, bijvoorbeeld doordat de hacker op een forum opschept over zijn hack.[128]

Dit is met name een probleem wanneer een partij 'weet' dat gegevens die in de procedure een doorslaggevende rol spelen, vals zijn maar in bewijsnood komt omdat het niet eenvoudig te bewijzen is. In dat geval kan en zal een partij namelijk ook geen verweer voeren omdat hij weet dat hij zijn verweer onvoldoende kan motiveren. Zo zal het vooral in termen van toegang en kosten lastig zijn wanneer je wilt bewijzen dat bijvoorbeeld een email vals is terwijl je voor het bewijs gebruik wilt maken van deze door jou verwijderde email op het emailaccount van je werkgever waartegen je verweer voert of zogenaamde freemail die bij derden in het buitenland is opgeslagen, zoals bij Gmail of Hotmail.[129] Het probleem ligt dan vooral in het feit dat het technisch terughalen waarschijnlijk nog wel mogelijk is maar dat daarvoor wel aanzienlijke kosten gemaakt moeten worden. Bij freemail zal het tevens een probleem zijn om juridisch toegang te krijgen tot de servers van bijvoorbeeld Microsoft of Google die zich veelal in de Verenigde Staten bevinden. Het bijkomende probleem is vaak dat je niet alleen naar een email zoekt maar ook naar de context daarvan en hoe langer het feit geleden is, hoe moeilijker het zal zijn gericht te zoeken.[130]

De wetgever heeft in het civiele recht geen maatstaf opgenomen voor het waarderen van bewijs. De rechter mag, behoudens wettelijke uitzonderingen, zelf bepalen welke waarde hij aan een bewijsmiddel toekent en wanneer het bewijs is geleverd.[131] In de literatuur wordt

[128] Zie bijvoorbeeld de 17-jarige hacker die in 2012 bijna het hele KPN-netwerk binnen wist te dringen maar vooral gepakt werd doordat hij hierover opschepte tegen een Zuid-Koreaanse student (Volkskrant 28/04/2012).
[129] Dat email wordt verwijderd is niet ongewoon omdat emailaccounts een maximale opslagcapaciteit hebben. In dit geval heb je ook weinig aan IP-adressen en verkeersgegevens, omdat je echt naar de inhoud op zoek bent.
[130] Zowel technisch (mogelijk is het al overschreven) als de zoekopdracht zelf. Jij zal immers moeten aangeven waar je naar op zoek en liefst zo gericht mogelijk (datum, trefwoord titel, etc.).
[131] In de literatuur wordt wel gesteld dat er niet één maatstaf is omdat ook de omstandigheden van het geval een rol kunnen spelen, zoals de aard van het geschil, de mate waarin bewijs geleverd kan worden (incest, letselschade) en het gewicht van de daarbij betrokken wederzijdse belangen. Zie o.m. Giesen 2001 (diss.), p. 56; De Bock 2011 (diss.), p. 205 en de daar aangehaalde literatuur en jurisprudentie.

algemeen aangenomen dat de rechter voor het vaststellen van de feiten in beginsel een redelijke mate van zekerheid moet hebben.[132]

Giesen heeft de bewijswaarderingsmaatstaf proberen te kwantificeren en stelde deze redelijke mate van zekerheid op ongeveer 75%.[133] Hij kwam echter ook tot de conclusie dat deze kwantificering ons niet veel verder brengt. Mede omdat er geen nadere geobjectiveerde invulling kan worden gegeven en het nagenoeg onmogelijk is om vast te stellen of alle rechters het over dezelfde mate van waarschijnlijkheid hebben.[134] De meest recente waarderingsmaatstaf komt van De Bock. Zij onderscheidt, deels in navolging van Schum, vier ijkpunten om te komen tot een verantwoorde eindbeslissing, die zij aanduidt als een intersubjectieve bewijswaarderingsmaatstaf: relevantie, kwaliteit, reikwijdte en de alternatieve hypothese.[135] Op basis van deze ijkpunten komt zij tot de volgende bewijswaarderings-maatstaf: 'Een feit is voor de civiele rechter bewezen wanneer uit de beschikbare bewijsmiddelen redelijkerwijs kan worden afgeleid dat het feit zich heeft voorgedaan, en uit die bewijsmiddelen niet even goed kan worden afgeleid dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan, terwijl zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden, ontbreekt.'[136]

Voor het watermerk zou de invulling van deze maatstaf concreet betekenen dat de rechter uit een betrouwbaar watermerk redelijkerwijs kan afleiden dat het bestand aan de licentienemer toebehoort. Daarnaast mag de rechter uit het watermerk niet even goed afleiden dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan en zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden, ontbreekt. Ten aanzien van het gestelde feit zal een betrouwbaar watermerk daar in beginsel aan kunnen voldoen. Een verweer dat zich richt op alternatieve verklaringen richt zich immers niet op dit feit maar op de gevolgtrekking die de rechthebbende baseert op dit feit; namelijk dat hij degene is geweest die het bestand op internet heeft geplaatst. Dat bewijs kan het watermerk niet leveren. Dat verweer blijft altijd mogelijk maar zal zoals eerder besproken in de praktijk niet eenvoudig zijn in te roepen (zie par. 4.3.2).

Samenvattend is de rechter in beginsel vrij in de waardering van het watermerk als bewijsmiddel. Bij een gebrek aan een specifiek of analoog toepasbaar kader zal de rechter

[132] De Bock 2011 (diss.), p. 202; Snijders, Klaassen & Meijer 2007, p. 209; Giesen 2001 (diss.), p. 51; Hidma & Rutgers 2004 spreken enerzijds (p. 7) van een redelijke mate van zekerheid en anderzijds (p. 8) van het meer Common Law (Anglo-Amerikaans) georienteerde 'preponderance of probabilities' dat meer duidt op het uitgangspunt dat een gesteld feit eerder aannemelijk is dan niet.
[133] In de Verenigde Staten komen uit verschillende onderzoeken percentages tussen de 75-90%. Zie onder meer Kerkmeester 2004, p. 122. Saunders 2005, komt met een nog bredere range tussen de 30-99,99% .
[134] Giesen 2001 (diss.); 1999, p. 630); De Bock 2011 (diss.), p. 206. Zie voor dezelfde discussie in de Verenigde Staten Anderson, Schum & Twining 2005, p. 247.
[135] De Bock 2011 (p. 212) schrijft in haar dissertatie voornamelijk over het civiele recht, waar David Schum meer spreekt over het Amerikaanse systeem van strafrecht. Mij lijken de begrippen ook toepasbaar voor het Nederlandse strafrecht. D.A. Schum 2004 komt tot die centrale begrippen bij de waardering van bewijs; relevance, credibility en probative force.
[136] De Bock 2011, p. 218. Zie haar betoog vanaf par. 5.6, p. 210.

houvast kunnen zoeken bij de waardering van forensisch deskundigenonderzoek waarmee meer ervaring is opgedaan in met name de strafrechtpraktijk.[137] Watermerken komen dan in het domein van digitaal forensisch onderzoek en de daarvoor gestelde beoordelingscriteria. Voor de waardering van watermerken verwijs ik verder naar hoofdstuk 6.

4.2.3.2 Debat: de bewijswaarderingsmaatstaf van De Bock & watermerken

De Bock stelt in haar lezenswaardige proefschrift over het tussen waarheid en onzekerheid vaststellen van feiten in de civiele procedure onder meer dat de Nederlandse bewijswaarderingsmaatstaf, die een redelijke mate van zekerheid vereist, onvoldoende antwoord geeft op de vraag wanneer of onder welke voorwaarden de rechter kan vaststellen dat sprake is van een redelijke mate van zekerheid of van voldoende aannemelijkheid.[138] Terwijl de bewijswaarderingsmaatstaf volgens haar juist een hulpmiddel moet zijn waarmee zoveel mogelijk bereikt kan worden dat feiten die waar zijn door de rechter ook bewezen worden geacht en feiten die niet waar zijn door de rechter niet bewezen worden geacht.[139] Zij stelt zich dan ook tot doel om een inhoudelijke invulling te geven aan de bewijswaarderingsmaatstaf, zodat inzichtelijk gemaakt kan worden wanneer de rechter een feit bewezen kan en moet achten.[140] Zij positioneert deze bewijswaarderingsmaatstaf terecht in het uiteindelijke doel van het bewijsrecht om de rechter, in het belang van de waarheidsvinding, in staat te stellen zoveel mogelijk tot een correcte vaststelling van de relevante feiten te komen.[141]

Bij het formuleren van een nieuwe maatstaf gaat het volgens haar niet om elk subjectief element of elk element van interpretatie van de bewijsmiddelen te benoemen, maar om een verheldering van de vraag wat bedoeld wordt met een bepaalde mate van rechterlijke overtuiging, met andere woorden het intersubjectief maken van de bewijswaarderings-maatstaf. Alleen dan kan volgens haar duidelijk worden gemaakt waarom de rechter het bewijs van een feit wel of niet geleverd acht. Deze norm geldt voor alle andere rechterlijke beslissingen. Deze moeten zodanig gemotiveerd zijn, dat inzichtelijk is op welke gronden de rechter de beslissing heeft genomen.[142]

---

[137] Zie voor inzet van (partij-)deskundigen in zaken van auteursrechtinbreuk o.m. Hof ‘s-Gravenhage 29 juni 2010, ECLI:NL:GHSGR:2010:BN8145; Rb. ‘s-Gravenhage 19 september 2012, ECLI:NL:RBSGR:2012:BX8147; Hof ‘s-Gravenhage 15 november 2010, ECLI:NL:GHSGR:2010:BO3980 (FTD/Eyeworks).

[138] Ongeacht of die nu luidt ‘een redelijke mate van zekerheid’, ‘voldoende aannemelijk zijn’ of ‘in voldoende mate komen vast te staan’ De Bock 2011 (diss), p. 211. Zie par. 4.2.3.1.

[139] De Bock 2011 (diss), p. 190.

[140] De Bock 2011 (diss), p. 211. Zie voor ontwikkelingen en standpunten sindsdien o.m. de pre-adviezen van de NJV 2012 over Waarheid en waarheidsvinding in het recht.

[141] De Bock 2011 (diss), p. 190.

[142] De Bock 2011 (diss.), p. 212, onder verwijzing naar o.m. HR 17 november 2006, NJ 2006, 621; HR 9 juni 2006, NJ 2006, 327; HR 1 november 2002, NJ 2005, 281; HR 29 juni 2001, NJ 2001, 495; HR 16 oktober 1998, NJ 1999, 7.

Om de bewijswaarderingsmaatstaf inzichtelijk te maken maakt zij een vergelijking met de medische bewijsbeslissing (diagnose arts) waaruit afgeleid kan worden welke ijkpunten kunnen worden onderscheiden bij het nemen van een verantwoorde bewijsbeslissing.[143] De invulling van deze ijkpunten ontleent De Bock voor een belangrijk deel aan het werk van David A. Schum, die als de centrale begrippen bij de waardering van bewijs noemt relevance, credibility en probative force.[144] Voor een uitgebreide beschrijving verwijs ik graag naar haar proefschrift.

Op basis van deze ijkpunten komt zij tot de volgende bewijswaarderingsmaatstaf:[145]

> 'Een feit is voor de civiele rechter bewezen wanneer uit de beschikbare bewijsmiddelen redelijkerwijs kan worden afgeleid dat het feit zich heeft voorgedaan, en uit die bewijsmiddelen niet even goed kan worden afgeleid dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan, terwijl zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden, ontbreekt'.

Deze maatstaf zou volgens De Bock een hulpmiddel moeten zijn, waarmee zoveel mogelijk bereikt kan worden dat feiten die waar zijn, door de rechter ook bewezen worden geacht en feiten die niet waar zijn, door de rechter niet bewezen worden geacht. Bovendien zou met deze maatstaf duidelijk worden gemaakt waarom de rechter het bewijs van een feit wel of niet bewezen acht. De motivering die daar op volgt moet dan duidelijk maken op welke gronden deze beslissing is genomen. Het idee lijkt dat wanneer de rechter de drie onderdelen uit de maatstaf gemotiveerd in haar oordeel en uitspraak betrekt duidelijk wordt gemaakt waarom de rechter het bewijs van een feit wel of niet bewezen acht. Aan de hand van een casus met het watermerk als bewijsmiddel wordt eerst onderzocht hoe dit criterium in de praktijk zou uitwerken en of dit criterium een oplossing kan bieden voor de hiervoor door De Bock genoemde bezwaren tegen de huidige bewijswaarderingsmaatstaf, die een redelijke mate van zekerheid vereist . Daarna zal nader worden ingegaan op de maatstaf.

Wanneer deze maatstaf wordt ingevuld aan de hand van de vraag of het watermerk kan bewijzen dat het op internet aangetroffen bestand aan de licentienemer toebehoort, dan kan de maatstaf als volgt worden ingevuld.[146] Hierbij is buiten beschouwing gelaten dat ook bij het bewijzen van deze stelling meerdere bewijsmiddelen een rol kunnen spelen die de rechter in dat geval ook in dit oordeel zou moeten betrekken. Om het watermerk als bewijsmiddel

[143] Ter vergelijking is het vreemd dat in de medische opleiding wel en bij een juridische opleiding geen vak bestaat als besliskunde waar studeten leren welke ijkpunten van belang zijn bij het nemen van een verantwoorde bewijsbeslissing.
[144] De Bock verwijst op pagina 212 naar Schum 2004. In haar literatuurlijst komen echter alleen Schum 1994 en 2003 voor. De verwijzing naar Schum is overigens een keuze. Er zijn meerdere onderzoeken verricht die naar vergelijkbare elementen wijzen. Zie o.m. par. 6.4.
[145] De Bock 2011, p. 218. Zie haar betoog vanaf par. 5.6, p. 210.
[146] Zie inleiding 4.1. Vanuit een materieelrechtelijk perspectief kan het watermerk slechts bijdragen aan het bewijs door aan te tonen dat de licentienemer het bestand openbaar heeft gemaakt door bij te dragen aan het bewijs van de stelling dat het op internet aangetroffen bestand aan de licentienemer toebehoort.

centraal te kunnen stellen wordt uitgegaan van de situatie dat er geen andere bewijsmiddelen zijn.

Het feit dat het op internet aangetroffen bestand aan de licentienemer toebehoort, is voor de civiele rechter bewezen wanneer (a) uit de beschikbare bewijsmiddelen redelijkerwijs kan worden afgeleid dat dit feit zich heeft voorgedaan, (b) en uit die bewijsmiddelen niet even goed kan worden afgeleid dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan, (c) terwijl zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden, ontbreekt.

De eerste voorwaarde (a) dat uit de beschikbare bewijsmiddelen redelijkerwijs kan worden afgeleid dat het feit zich heeft voorgedaan, zal in de regel eenvoudig kunnen worden ingevuld. Wanneer de door de rechthebbende ingebrachte rapportage aantoont dat het op internet aangetroffen bestand een watermerk bevat waarin de gegevens van de gedaagde (licentienemer) zijn opgenomen, kan de rechter uit die rapportage redelijkerwijs afleiden dat het gestelde feit zich heeft voorgedaan. Een dergelijke oordeel veronderstelt dat de rechter, al dan niet naar aanleiding van stellingen van partijen, uiteindelijk voldoende vertrouwen heeft in het voorgestelde systeem van watermerken. Zonder dat oordeel zal hij uit het bewijs niet redelijkerwijs kunnen afleiden dat het gestelde feit zich heeft voorgedaan. De vraag waarom de rechter het bewijs van een feit wel of niet bewezen acht zal, zoals De Bock ook zelf stelt, vooral moeten blijken uit de motivering in de uitspraak zelf. Daarover later meer.

De tweede voorwaarde (b) dat uit die bewijsmiddelen niet even goed kan worden afgeleid dat hetgeen de wederpartij met betrekking tot dat feit stelt zich heeft voorgedaan hangt vanzelfsprekend samen met hetgeen de partij die het feit betwist hiertegenover stelt. De gedaagde kan in beginsel drie aannemelijke verweren voeren.[147] Ten eerste verweren die zich richten op de toelaatbaarheid van het watermerk als bewijsmiddel. Ten tweede verweren die erop gericht zijn de betrouwbaarheid van het watermerk aan te tasten en ten derde verweren die zich richten op de conclusie die de rechthebbende zal willen verbinden aan het feit dat het bestand aan de gedaagde of verdachte toebehoort (alternatieve verklaringen). De eerste twee verweren zullen samenhangen met de eerste voorwaarde (a). Uit watermerken die niet toelaatbaar of betrouwbaar zijn kan de rechter immers niet redelijkerwijs afleiden dat het feit zich heeft voorgedaan. De toewijsbaarheid van de alternatieve verklaring is sterk afhankelijk van de feiten en het bewijs dat die partij voor haar stelling kan leveren. Een gedaagde (licentienemer) die stelt te zijn gehackt maar dit niet kan bewijzen zal zijn stelling, die op zich waar kan zijn, niet gehonoreerd zien. Vanuit de context van de juridische waarheidsvinding strandt zijn stelling. Ook hier geldt dat de vraag waarom de rechter uit die bewijsmiddelen niet even goed de stelling van de gedaagde had kunnen afleiden vooral moeten blijken uit zijn motivering.

[147] Par. 4.2.2.

De derde en laatste voorwaarde houdt in dat (c) zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden, ontbreekt. De Bock geeft aan dat de rechter een bepaald verwachtingspatroon heeft over wat in het concrete geval aan bewijsmateriaal aanwezig moet zijn.[148] Als voorbeeld noemt zij een partij die bijvoorbeeld moet bewijzen dat hij letselschade heeft opgelopen omdat zijn wederpartij hem een klap heeft gegeven. De rechter zal volgens haar dan waarschijnlijk geen genoegen nemen met enkel een verklaring van een getuige dat sprake is van letselschade, omdat normaal gesproken iemand voor letselschade naar een arts gaat, zodat een medische verklaring mag worden verwacht. Wanneer die verklaring ontbreekt is het bewijsmateriaal qua omvang onvolledig en zal de rechter het bewijs volgens haar waarschijnlijk niet geleverd achten.[149] Hoewel ik begrijp dat De Bock deze voorwaarde apart noemt zal deze in de praktijk reeds betrokken worden bij de voorgaande voorwaarden. Voor de rechthebbende geldt immers dat wanneer hij het gestelde feit met het watermerk wil bewijzen verwacht mag worden dat de rapportage ingaat op de feiten die daarbij van belang zijn.[150] Denk daarbij aan punten die relevant zijn voor de betrouwbaarheid van het bewijs, zoals de vraag hoe groot de kans is op een fout-positief. Gebreken op relevante punten doen immers afbreuk aan de betrouwbaarheid van het bewijs. Dat geldt ook voor de eerder besproken situatie onder b, dat een gedaagde (licentienemer) die stelt te zijn gehackt bewijs zal moeten leveren voor deze stelling. Wanneer hij het bewijs niet kan leveren dan zal zijn stelling, die op zich waar kan zijn, door de rechter niet aanvaard worden. Als bewijsmateriaal dat redelijkerwijs verwacht mocht worden ontbreekt mag worden aangenomen dat de rechter de onder a en b bedoelde feiten ook niet kan afleiden. Niettemin is het een vraag die bij de totale beoordeling betrokken dient te worden. Wanneer een rechthebbende zijn producten beschermt met een watermerk en iemand aanspreekt zonder het watermerk als bewijsmiddel te gebruiken, dan is het niet ondenkbaar dat de wederpartij de stelling betrekt dat het watermerk een middel is dat redelijkerwijs verwacht mocht worden. In hoeverre dat beroep een kans van slagen heeft hangt samen met de omstandigheden van het geval.

Deze maatstaf zou volgens De Bock een hulpmiddel moeten zijn, waarmee zoveel mogelijk bereikt kan worden dat feiten die waar zijn, door de rechter ook bewezen worden geacht en feiten die niet waar zijn, door de rechter niet bewezen worden geacht. De door De Bock genoemde voorwaarden maken het naar mijn mening noch afzonderlijk noch in zijn geheel bereikbaar dat de rechter feiten die waar zijn ook bewezen acht en feiten die niet waar zijn, niet bewezen acht. Een hulpmiddel is het naar mijn mening wel, omdat het de rechter een beter toetsingskader geeft dan tot op heden het geval was. Het biedt echter geen hulpmiddel waarmee zoveel mogelijk bereikt kan worden dat de rechter een beslissing neemt op grond

[148] De Bock 2011 (diss.), p. 215.
[149] De Bock 2011 (diss.), p. 216 merkt op dat de rechter - om valkuilen te vermijden - er goed aan doet om vóór de definitieve bewijsbeslissing een partij te confronteren met haar opvatting over ontbrekend bewijsmateriaal, zodat duidelijk kan worden of er een gerechtvaardigde reden is dat het door de rechter verwachte bewijsmateriaal ontbreekt.
[150] Zie par. 4.2.2. en hoofdstuk 6.2 en 6.3. Denk daarbij ook aan ander bewijs dat de rechthebbende kan leveren, zoals bewijs dat aantoont dat (bv. d.m.v. betalingsbewijzen) en wanneer de licentie is gesloten en wat de achtergrond ervan is (gebruik, distributie, review, etc.).

van de juiste feiten. Daarvoor ontbreekt naar mijn mening de aandacht voor psychologische valkuilen. Ik kom daar later nog op terug.

De door De Bock genoemde voorwaarden maken naar mijn mening noch afzonderlijk noch in zijn geheel duidelijk waarom de rechter het bewijs van een feit wel of niet bewezen acht. Althans niet meer of minder dan onder de huidige bewijswaarderingsmaatstaf. Ook De Bock ontkomt namelijk niet aan het geven van een invulling die erop neer komt dat de rechter tot een redelijk oordeel moet komen. Het antwoord op de vraag waarom de rechter het bewijs van een feit wel of niet bewezen acht zal te vinden moeten zijn in de motivering van zijn uitspraak. Daarbij kunnen de door haar genoemde voorwaarden behulpzaam zijn, omdat deze vragen oproepen die mogelijk duidelijker maken op welke gronden de rechter tot zijn oordeel gekomen is. De Bock voegt met haar maatstaf vragen toe die afzonderlijke aandacht verdienen bij het vaststellen van feiten. De maatstaf geeft in die zin meer houvast voor de beoordeling van feiten en de motivering dan tot nu toe het geval was. Het betreft echter vooral een intern perspectief van de rechter. De rechter wordt hiermee een kader geboden om zijn eigen gedachten te structureren om zodoende de feiten die waar zijn ook bewezen te achten en feiten die niet waar zijn, niet bewezen te achten. De motivering die dit proces ook voor anderen inzichtelijk moet maken blijft buiten haar beschouwing. Zij richt zich met haar maatstaf dan ook vooral tot de rechter. Dat zij niet verder ingaat op de motivering is te rechtvaardigen vanuit de gedachte dat er nu eenmaal keuzes gemaakt moeten worden. Een nadere analyse van de motivering van rechtspraak vraagt in dit licht immers om een andere en meer uitgebreide benadering. Zie daarvoor bijvoorbeeld in het strafrecht, het Project Motiveringsverbetering in Strafvonnissen (Promis) dat tien jaar geleden al is gestart.[151]

Voor een nadere beoordeling van haar maatstaf is het voorts van belang om inzicht te krijgen in de wijze waarop rechters tot hun beslissingen komen. In 2008 heeft Visser voor het eerst in Nederland een poging gedaan om inzicht te krijgen in de vraag hoe de rechter geschillen op het gebied van de intellectuele eigendom (IE) in de praktijk beslist.[152] Daarbij stelde hij vragen naar de factoren die van belang zijn voor een rechter in IE-inbreukzaken en hoe hij of zij tot zijn of haar beslissing komt. Hoewel het denkbaar is dat rechters in andere dan IE-zaken op een andere wijze tot een beslissing komen lijkt mij dat op voorhand niet aannemelijk. Het onderzoek van Visser geeft namelijk vooral een beeld van de wijze waarop

[151] Onderzoek (2014) naar Promis (De Groot-van Leeuwen e.a. 2015) wijst uit ‘dat zowel in de ervaringen van procesdeelnemers als bij het brede publiek het geven van meer informatie in de vonnissen vormgegeven op de Promis-wijze leidt tot meer inzicht en meer acceptatie’ (p. 5). Het onderzoek wijst tevens uit dat rechters die volgens Promis een vonnis schrijven, uitgebreider motiveren en meer gestructureerd aangeven hoe zij tot een oordeel komen. Dat leidt er bij de lezer toe dat hij meer inzicht krijgt in de wijze waarop de rechter tot zijn oordeel is gekomen. Deze begrijpelijkere vonnissen leiden tevens tot meer acceptatie van de bewezenverklaring. Zie ook verkort (red.) NJB 2015/7, nr. 398, p. 481: 'Uitgebreid motiveren leidt tot meer begrip vonnissen’.

[152] Visser 2008, p. 1918. Zie voor de methodologie, ook p. 1918. Visser interviewde begin 2008 zeventien rechters met veel ervaring in IE-zaken. De vragenlijst en de gesprekken hebben vooral betrekking op de beslissing van IE-zaken in kort geding in eerste instantie. Het onderzoek heeft zich beperkt tot het merkenrecht, het handelsnaamrecht, het auteursrecht, het modellenrecht en de slaafse nabootsing en heeft derhalve geen betrekking op het octrooirecht. Visser maakt bij de verslaglegging veel gebruik van citaten van rechters. Deze zal ik, voor zover relevant, in voetnoten plaatsen.

de rechters in de praktijk omgaan met criteria uit voornamelijk de rechtspraak. Tegen die achtergrond is er weinig reden om aan te nemen dat rechters in andere civielrechtelijke rechtsgebieden op een totaal andere wijze omgaan met criteria die in de jurisprudentie zijn ontwikkeld. Van belang is wel om op te merken dat het een heel specifiek onderzoek is onder een beperkte groep rechters. Visser benoemt het dan ook terecht in termen van een 'poging om zicht te krijgen'. Grotere studies zouden meer zekerheid kunnen geven. Al sluiten de resultaten uit zijn onderzoek aan bij andere studies die zijn verricht naar de wijze waarop rechters tot een beslissing komen.[153]

In het onderzoek van Visser komt de vraag naar voren hoe rechters omgaan met de verschillende (inbreuk)criteria uit de IE-literatuur of IE-jurisprudentie. Tegen die achtergrond kan worden gekeken naar de vraag wat een rechter in de praktijk doet met een maatstaf zoals ook De Bock die introduceert. Visser merkt op dat over het nut van de verschillende criteria verschillend wordt gedacht.[154] Rechters lijken vooral steun te vinden in de criteria om hun oordeel te kunnen motiveren.[155] Zij lijken zich er tegelijk van bewust dat terminologie de basis verhult waarop zij tot hun oordeel komen.[156] Dit komt overeen met de uitspraak van Verkade in zijn annotatie onder het Decaux/Mediamax-arrest, waarin hij stelt dat advocaten en feitenrechters bij hun stellingnamen omtrent de aan- of afwezigheid van een te grote gelijkenis, naar vermogen lippendienst moeten bewijzen aan de onderscheiden inbreukregels en subcriteria voor bescherming van produktvormgeving'.[157] Volgens Visser onderschrijven de meeste rechters deze stelling wel, maar vinden zij de term 'lippendienst' te negatief.[158] Visser beschrijft dat het volgens enkele rechters bij de beoordeling van IE-inbreukzaken uiteindelijk gaat om basale rechtspolitieke overwegingen, zoals de vraag wat eigendom is en wat er gedeeld moet worden.[159] Uiteindelijk gaat het volgens de meeste rechters om (al dan niet) 'onbetamelijk gedrag jegens een ander'. Of anders gezegd om de beoordeling van een fatsoensnorm, die niet veel verschilt van de onrechtmatige daad, waarbij het noodzakelijkerwijs gaat om subjectieve en deels gevoelsmatige beoordeling.[160]

Toch merkt Visser op dat de rechters wel enige steun vinden in de criteria die in de rechtspraak zijn ontwikkeld.[161] Met name omdat criteria iets zeggen over het doel van de

[153] Zie par. 6.4.
[154] Visser 2008, p. 1923.
[155] Visser 2008, p. 1923: 'je moet wel wat hebben om het te motiveren';
[156] Visser 2008, p. 1923: 'de terminologie verhult de basis waarop je tot je oordeel komt'; 'De kreten die bestaan die gebruik je gewoon.'
[157] Verkade in zijn noot onder HR 29 december 1995, NJ 1996, 546 (Decaux/Mediamax; stadsmeubilair),
[158] Visser 2008, p. 1925: 'Eén rechter merkt op: 'alles wat de feitenrechter doet, is in principe goed als hij maar lippendienst bewijst aan het inbreukcriterium en het een beetje te volgen is'.'
[159] Visser 2008, p. 1925.
[160] Visser 2008, p. 1925. Vgl ook Scholten 1974, p. 130.De rechter vormt volgens Scholten niet alleen een oordeel, maar doet vooral recht: 'Het is niet een wetenschappelijk oordeel, het is een wilsverklaring: zo moet het. Het is tenslotte een sprong, gelijk iedere daad, ieder zedelijk oordeel dat is.'
[161] Visser 2008, p. 1923. 'Je hebt wat meer houvast om het rijtje af te lopen.'; 'Iets meer handvatten.'; 'Ze dwingen je om je rekenschap te geven van de factoren die van belang zijn.'; 'Je kunt er een denkpatroon aan ontlenen .'; 'Je denkt in categorieën en die geven wel enige sturing.'

bescherming en rechters helpen om hun denken te kanaliseren. Criteria geven iets meer handvatten en daarmee houvast om rekenschap te geven van factoren die van belang zijn.

Criteria normeren het handelen van de rechter. Zoals een rechter in een interview met Visser opmerkt kan een opvatting waar geen maatstaf voor te vinden is niet door de rechter worden volgehouden.[162] Het kan ook voorkomen dat de rechter moet concluderen dat hij zijn oorspronkelijke oordeel niet op papier krijgt omdat de feiten niet passen bij de gestelde criteria.[163] Visser merkt op dat verschillende rechters hebben aangegeven weleens een onjuiste motivering te hebben gebruikt voor een overigens juiste beslissing. Bijvoorbeeld door merkenrechtelijke criteria te gebruiken in een handelsnaamzaak of door een bepaald voortbrengsel niet beschermd te achtten, waardoor zij aan de inbreukvraag niet toekwamen, terwijl zij eigenlijk het voortbrengsel wel beschermd hadden moeten achtten, om vervolgens geen inbreuk aan te nemen. Volgens Visser benoemden de rechters deze voorvallen in de regel als 'bedrijfsongevallen' die in de kortgedingpraktijk nu eenmaal voorkomen.[164] Het is een open vraag of dit enkel bedrijfsongevallen zijn die in de kortgedingpraktijk voorkomen. Het is tevens de vraag of dit ook daadwerkelijk in alle gevallen een probleem is. De redenering die rechters er hier op nahouden is immers dat zij recht proberen te doen aan de situatie waar zij voor gesteld zijn. Zie in dat kader ook de Hoge Raad die in het arrest Jan de Waard, die na het ongewone pleidooi van Martens[165], tot het oordeel kwam dat er ruimte was voor cassatie in een zaak die in hoge mate feitelijk was.[166] Het doen van recht, in termen van het wijzen van een uitspraak die door partijen in redelijkheid kan worden aanvaard, lijkt mij het uiteindelijke doel van de rechtspraak. Of zoals De Bock het zelf ook formuleert: 'het resultaat van de oordeelsvorming moet immers een aanvaardbare beslissing zijn die past in het rechtssysteem en voldoet aan de eisen van rechtvaardigheid.'[167] Tegen die achtergrond hoeft het niet in alle gevallen daadwerkelijk een probleem te zijn dat er bedrijfsongevallen plaatsvinden. Een dergelijk bedrijfsongeval zou er in de wetenschappelijke praktijk toe moeten leiden dat hierin een aanleiding kan worden gevonden die de vraag rechtvaardigt of het bestaande recht niet moet worden bijgesteld, verfijnd of verworpen.[168]

De rechters uit het onderzoek van Visser lijken de criteria voornamelijk te gebruiken als denkkader om hun oordeel te kunnen motiveren. De criteria dienen in die zin dan ook vooral als de verantwoording van de beslissing, maar zeggen niet hoe de rechter tot zijn beslissing

[162] Visser 2008, p. 1923.
[163] Visser 2008, p. 1923: 'Ik krijg het niet op papier'.
[164] Visser 2008, p. 1923.
[165] 'Omdat in deze zaak, naar mijn overtuiging onrecht dreigt te geschieden, althans omdat daarin, naar mijn overtuiging, tot nu toe, door samenloop van omstandigheden, geen recht is gedaan.'
[166] HR 26 maart 1971, NJ 1971, 262 (Jan de Waard). Zie ook Scholten in zijn noot onder dit arrest: 'Voor een cassatiepleitnota is zij ongewoon, namelijk in hoge mate feitelijk; zo voortreffelijk echter dat wie haar gelezen heeft, zich gedwongen voelt te zoeken hoe in deze zaak cassatie kan worden bereikt.' De pleitnota van Martens i gepubliceerd in Verkeersrecht 1972, p. 272.
[167] De Bock 2011, p. 6 of zoals De Groot (2008, p. 2) stelt: 'Een rechterlijke beslissing moet begrijpelijk zijn met het hoofd, invoelbaar met het hart, en uitvoerbaar met de benen.'
[168] Zie voor de verschillende tussen het vaststellen van feiten in het recht en de wetenschap in het algemeen De Bock 2011 (diss.), p. 191 en Vranken (2014) in het zijn Algemeen Deel.

komt.[169] Visser merkt op dat de criteria volgens de rechters vaak wel een denkrichting aangeven, maar ook veel ruimte openlaten.[170] Eén rechter merkt op dat de wetenschap moet blijven zoeken naar sterker meetbare houvasten, omdat iets 'steeds weer van een ander etiketje te voorzien dat in feite dezelfde emotie is', het IE-recht niet veel zal verder brengen.[171] Aangenomen mag dan ook worden dat rechters ook enige steun vinden in de criteria die in de literatuur worden ontwikkeld. Al zullen in de praktijk criteria die in de jurisprudentie zijn ontwikkeld de sterkste invloed hebben op de beslissing en de motivering van de rechter.

De Groot merkt in de bespreking van de dissertatie van De Bock op dat het denkbaar is dat te betogen is dat de bewijsmaatstaf die de civiele rechter naar huidig recht noopt tot soortgelijke afwegingen, of dat de door De Bock voorgestane bewijswaarderingsmaatstaf in de rechtspraktijk even subjectief of objectief is in te vullen als de huidige bewijswaarderingsmaatstaf, maar dat zij daar niet nader op in zal gaan.[172] Dat is jammer omdat in het antwoord op die vraag besloten ligt of het door De Bock voorgestelde criterium het recht weer verder brengt. Niet in de laatste plaats omdat, zoals al eerder is opgemerkt, rechters wel enige steun vinden in de criteria. Met name omdat criteria iets zeggen over het doel van de bescherming en rechters helpen om hun denken te kanaliseren. Zij geven iets meer handvatten en daarmee houvast om rekenschap te geven van factoren die van belang zijn. Het criterium van De Bock brengt zoals ik eerder aangaf het recht in die zin wel degelijk een stapje verder. Zelfs als de bewijsmaatstaf de civiele rechter naar huidig recht noopt tot soortgelijke afwegingen dan nog draagt de maatstaf bij aan de denkkaders van de rechters of geeft zij handvatten waarop de rechter zijn oordeel kan baseren en motiveren. In die zin kunnen de criteria bijdragen aan een betere verantwoording van de beslissing. Zij biedt echter beperkt handvatten om duidelijk te krijgen, op welke wijze de rechter tot zijn beslissing komt. De vraag is dan ook of er veel sterker meetbare houvasten in het recht te vinden zijn.[173]

Voor de vraag hoe rechters tot hun beslissing komen moeten wij uit de rechtswetenschappelijke literatuur stappen. In Nederland hebben de psychologen Crombag, Van Koppen & Wagenaar in 1993 in hun boek Dubieuze zaken aandacht gevraagd voor de psychologie van strafrechtelijk bewijs.[174] Naar aanleiding van een aantal rechterlijke dwalingen, zoals de Puttense Moordzaak en Lucia de B. is de aandacht voor de wijze waarop rechters, maar ook het OM en de politie tot bepaalde beslissingen komen, toegenomen.[175] De belangrijkste uitkomst is dat er te weinig aandacht is geweest voor een alternatieve hypothese in relatie tot het bewijs.[176] Of anders gezegd er is te weinig aandacht geweest voor een andere verklaring

[169] Visser 2008, p. 1924.
[170] Visser 2008, p. 1924.
[171] Visser 2008, p. 1924.
[172] De Groot 2012, p. 63.
[173] Zie ook Visser 2011b, p. 323. (motiveren) Visser concludeert dat beslissingen in IE-zaken naar zijn overtuiging inderdaad in hoge mate subjectief zijn en wij daar mogelijk maar mee hebben te leven.
[174] Zie verder par. 6.4.
[175] Zie par. 6.4. Ook voor de verwijzingen naar deze arresten.
[176] Zie voor de uitkomsten naar aanleiding van Schiedammer Parkmoord, het rapport Posthumus 2005.

voor hetzelfde feitencomplex. Er is geen reden om aan te nemen dat dezelfde problemen ten aanzien van bewijswaardering zich niet in het civiel recht voordoen.[177] De Bock hevelt, zonder daar expliciet naar te verwijzen, de lessen die uit het strafrecht worden getrokken over naar het civiel recht.[178] Zij heeft in haar nieuwe criterium aandacht voor de alternatieve hypothese of anders gezegd voor een andere verklaring voor hetzelfde feitencomplex.[179] Daarmee draagt zij bij aan de waarheidsvinding door de rechter bij het beoordelen van het bewijs deze vragen expliciet te laten stellen en in haar uitspraak te motiveren.

De Groot stelt terecht de vraag of de door De Bock voorgestane bewijswaarderingsmaatstaf in de rechtspraktijk niet even subjectief of objectief is in te vullen als de huidige bewijswaarderingsmaatstaf.[180] Ik vrees van wel. Criteria in het recht zijn vaag en de beoordeling daarvan waarschijnlijk altijd subjectief en geven weinig tot geen houvast voor een beslissing. Daar is, zoals Visser ook ten aanzien van IE-criteria concludeert, mogelijk niet zoveel aan te doen.[181] Maar het is, zoals hij ook stelt, wel belangrijk om er steeds rekening mee te houden, om het risico te voorkomen dat de (IE-)gemeenschap zich verliest in de eigen mandarijnenwetenschap.[182] Dat dreigt volgens Visser vooral wanneer de vorm van de meest actuele criteria belangijker wordt gevonden dan de inhoud, te weten of en hoe een beslissing nu echt verklaard of voorspeld kan worden. Hij acht het daarom vooral van belang om te blijven zoeken naar de factoren die in de praktijk, terecht of ten onrechte, van invloed zijn op de beslissing. In de juridische literatuur hebben juristen de rechterlijke beslissing onder verwijzing naar Scholten veelal beschreven als een ongrijpbaar moment. De laatste jaren is vooral vanwege de gerechtelijke dwalingen in het strafrecht meer aandacht voor de wijze waarop rechters tot hun beslissing komen.[183] Deze dwalingen zijn in de literatuur mede toegeschreven aan verschillende valkuilen waaraan mensen blootstaan bij het nemen van beslissingen.[184] De maatstaf van De Bock houdt naar mijn mening daar te weinig rekening mee. De Bock beschrijft vooral wanneer de rechter een feit bewezen kan achten, maar geeft

[177] Zie o.m. Giard 2011, ook voor voorbeelden in het civiele recht.
[178] De Bock verwijst slechts in een voetnoot naar de ontwikkelingen in strafrecht. Zij wijst er daarbij op dat dit een van de punten is waarop de strafrechtelijke bewijsbeslissing verschilt van de civielrechtelijke. De strafrechter moet niet alleen de hypothese van het OM en die van de verdediging toetsen, maar 'ook rekening houden met de mogelijkheid dat er in werkelijkheid iets is gebeurd dat door het openbaar ministerie noch door de verdediging naar voren is gebracht.'[178] De Bock 2011 (diss.), p. 217, noot 89 onder verwijzing naar Wagenaar, Van Koppen en Israëls (2009) p. 1447.
[179] De Bock 2011 (diss.), p. 219.
[180] De Groot 2012, p. 63.
[181] Visser 2011b, p. 325.
[182] Idem..
[183] Met de term rechterlijke dwaling wordt hier verwezen naar een verkeerde vaststelling van feiten en niet op rechtskwesties waartegen in beginsel wel cassatie openstaat. Rechterlijke dwaling vormen met name in die zaken een probleem waarin een verkeerde vaststelling van feiten leidt tot een onjuiste uitspraak, dat wil zeggen dat de verdachte ten onrechte wordt veroordeeld (vals positief) of ten onrechte wordt vrijgesproken (vals negatief). Bekende voorbeelden van gerechtelijke dwalingen zijn de Puttense Moordzaak (Hof Leeuwarden 24 april 2002, ECLI:NL:GHLEE:2002:AE1877, NS 2002, 182), Schiedammer Parkmoord (Hof Amsterdam 4 mei 2006, ECLI:NL:GHAMS:2006:AW8270) en Lucia de B. (Hof Arnhem 14 april 2010, ECLI:NL:GHARN:2010:BM0876, NJ 2010, 363 m. nt. P.A.M. Mevis).
[184] Zie voor een overzicht van de literatuur over de discussie over de wijze waarop rechters tot hun oordeel komen en de juridische waarheidsvinding o.m. Rozemond 2010. Zie voor bewijswaardering en psychologische inzichten in het civiele recht Enneking, Giesen & Rijnhout 2013. Zie verder par. 6.4.

niet aan hoe hij tot de juiste beslissing komt. Dat wil zeggen een beslissing waarbij hij de eerder genoemde valkuilen zoveel mogelijk vermijdt. Juist daar is nog de meeste winst te halen voor het waarderen van het bewijs.[185] Mogelijk ligt de winst van het nieuwe criterium dat De Bock introduceert ook wel daarin dat met deze bijdrage het einde in zicht is gekomen van de bijdrage die juristen op dit moment kunnen leveren aan het formuleren van een bewijswaarderingsmaatstraf. Niet in de laatste plaats omdat het proces van waarheidsvinding een multidisciplinair vraagstuk is dat uit veel meer wetenschapsgebieden en praktische domeinen bestaat dan enkel het recht.[186] Zo is er vanuit de psychologie veel aandacht voor de valkuilen die mensen tegenkomen bij het nemen van beslissingen en wordt er inmiddels vanuit verschillende disciplines aan modellen gewerkt om deze valkuilen te vermijden en ook aandacht te hebben voor alternatieve hypothesen.[187]

4.2.3.3 De deskundige als betrouwbare informant

De rechter is vrij anderen bij zijn oordeelsvorming te betrekken, maar het is het wezen van de rechtspraak dat de rechter een oordeel vormt en dat hij de aan hem opgedragen taak niet mag delegeren.[188] Bij technisch bewijs is het niet ongebruikelijk dat de rechter zich door een deskundige laat voorlichten door middel van een deskundigenverslag of getuigenis ter zitting.[189] In de meeste gevallen brengt echter ten minste één partij een (verslag van) deskundige in.[190] Het is dan aan de wederpartij om zijn eigen bevindingen daarover kenbaar te maken. Het staat de rechter altijd vrij een deskundige in te schakelen om hem onafhankelijk voor te lichten. Er is geen reden om aan te nemen dat dit bij watermerken anders is of anders zou moeten zijn.

Vanwege de grote beoordelingsvrijheid van de rechter kan hij in beginsel iedereen die hij deskundig acht benoemen en horen. In het Nederlandse strafrecht zijn daarvoor in de loop der tijd een aantal algemene criteria geformuleerd en is met de invoering van de Wet deskundige in strafzaken in 2010 de taak van de deskundige duidelijker in de wet verankerd. Tevens is er

[185] Zie ook par. 6.4.

[186] Zie ook Twining 2003; Giard 2009, p. 42. In die zin is het bijzonder dat aan medische faculteiten wel medische besliskunde wordt gedoceerd, maar er geen vak juridisch besliskunde is.

[187] www.nwo.nl/forensicscience (opgestart november 2010); KNAW, Bèta in crime. Wetenschappelijk bewijs in rechtszaken, symposium, 11 juni 2012. Een aantal in dit onderzoek meer summier behandelde onderwerpen zoals bewijswaardering op basis van bayesiaanse statistiek en de likelyhood ratio worden in twee onderzoeken nader uitgewerkt (o.m. het onderzoek(voorstel) van M. Sjerps en het onderzoek van B. Verheij. Daarnaast is er ook een project inzake E-Discovery in electronic data van M. de Rijke).

[188] Parl. Gesch. Bewijsrecht 1988, p. 316. Zie verder o.m. EHRM 18 maart 1997, NJ 1998, 278, m.nt. Snijders (Mantovanelli/Frankrijk). Het is aan het beleid van de feitenrechter overgelaten om te beslissen of hij wil overgaan tot het benoemen van een deskundige. Zie o.m. HR 16 april 1999, ECLI:NL:HR:1999:ZC2887, NJ 1999, 666, m.nt. P. Clausing..

[189] Art. 194 e.v.Rv. Denk hierbij bijv. aan merk (HR 20 november 2009, ECLI:NL:HR:2009:BJ6999 (Lego/Mega Brands), bouw- (bv. ECLI:NL:RBROT:2007:BG2640), letsel- (bv. ECLI:NL:GHSGR:2011:BP8571) of arbeidszaken (bv. ECLI:NL:GHSHE:2012:BX8474). De door de rechter benoemde deskundige wordt betaald uit de voorschotregeling, die door eisende partij ter griffie wordt gestort (art. 195 Rv). De maximumtarieven zijn vastgelegd in artikel 2 van het Besluit griffierechten burgerlijke zaken.

[190] Zie voor de inzet van deskundigen evenals het onderscheid tussen de door de rechter benoemde deskundige en de partij-deskundige, o.m. De Groot 2008 (diss.). In dit onderzoek wordt in overeenstemming met het gebruik door de Hoge Raad in beide gevallen gesproken van een deskundigenonderzoek.

een landelijk openbaar deskundigenregister opgezet, het Nederlands Register Gerechtelijke Deskundigen (NRGD).[191] De reikwijdte van het NRGD is beperkt tot het strafrecht. Inmiddels houdt een werkgroep zich momenteel bezig met een uitbreiding naar deskundigen die opereren in het civiele recht en het bestuursrecht.[192] Inmiddels bestaat er al wel een gedragscode voor gerechtelijk deskundigen in civielrechtelijke zaken.[193] Vragen die spelen ten aanzien van de deskundigheid van de deskundige verschillen of zouden in wezen niet moeten verschillen met de eisen die in het strafrecht aan deskundigen worden gesteld. Zie voor een verdere inhoudelijke bespreking van de kwaliteit van het onderzoek en de deskundige paragraaf 4.4.3.2.[194]

De deskundige behoort een optimale bijdrage te leveren aan een zo waarheidsgetrouw mogelijke beslissing.[195] Hij draagt hieraan bij door de vaststelling van betwiste of ambtshalve door de rechter te onderzoeken hypothesen, maar ook door conclusies te trekken en de rechter voor te lichten op domeinen waarop de rechter niet over de nodige deskundigheid beschikt.[196] Voor de aan de deskundige te stellen vragen is het van belang welke verweren ten aanzien van de watermerktechniek mogelijk zijn.[197] De rechter kan met de hulp van de deskundige een hogere graad van zekerheid verkrijgen of niet. Voor het onderzoek dat in opdracht van de rechter plaatsvindt geldt in beginsel ook dat medewerking is vereist van de rechthebbende in die zin dat hij toegang moet geven tot het watermerkproces. Hij is hiertoe verplicht op grond van art. 21 en 22 Rv, waarin de waarheids- en inlichtingenplicht is opgenomen, maar meer specifiek op grond van art. 198 Rv, waarin uitdrukkelijk is bepaald dat partijen verplicht zijn aan een onderzoek door deskundigen mee te werken (lid 3). Wanneer niet aan deze verplichting wordt voldaan dan kan de rechter daaruit de gevolgtrekking maken die hij geraden acht (lid 4).[198] Ondanks dat de inbreng van de deskundige van groot belang is bij de rechterlijke oordeelsvorming is het sinds 1923 niet meer mogelijk hem te wraken.[199] Ook wordt hij niet langer beëdigd.[200]

[191] Naast het NRGD bestaat er ook een landelijk register voor gerechtelijk deskundigen (LRGD) en een deskundigenregister van en voor de rechterlijke macht voor civielrechtelijke en bestuursrechtelijke rechtspleging (DIX). Zie verder par. 4.4.3.2.
[192] http://www.nrgd.nl/nrgd/speelveld/projectennrgd/. Zie voor opties tot vernieuwing van deskundigen in civiele zaken o.m. Krans & Santing-Wubs 2012.
[193] Versie 3.7, januari 2012. De gedragscode is opgesteld op verzoek van de Raad voor de rechtspraak en onder de verantwoordelijkheid van de landelijke voorzittersoverleggen van de rechtbanken en gerechtshoven. Deze is geënt op de gedragscode van het Nederlands Register Gerechtelijk Deskundigen (NRGD), omdat wordt beoogd op termijn te komen tot één universele gedragscode voor gerechtelijk deskundigen. Zie par. 4.4.3.2.
[194] Zie verder het Model deskundigenbericht behorend bij de Leidraad deskundigen (in civiele zaken) op www.rechtspaak.nl.
[195] Zie o.m. De Groot 2008 (diss.), p. 6.
[196] Asser 2013 p. 189; Schwartzenberg 2013, p. 216.
[197] De meest aannemelijke verweren worden behandeld in par. 6.3.2.
[198] Zie voor de medewerking van partijen aan het deskundigenonderzoek uitgebreid De Groot 2008 (diss.)
[199] Verkerk 2007.
[200] Zie Parl. Gesch. Bewijsrecht p. 316.

De waardering van het aan het verhoor of bericht van de deskundige te ontlenen bewijs is niet dwingend. Het verhoor of bericht heeft dus eveneens vrije bewijskracht.[201] Schriftelijke verklaringen van getuigen, waaronder ook expertiserapporten, hebben in het Nederlandse bewijsrecht geen bijzondere status.[202] De rechter is, in tegenstelling tot bijvoorbeeld bij de waardering van getuigenverklaringen, niet geheel vrij in de waardering van de zienswijze van een door hem benoemde deskundige.[203] De Hoge Raad stelt bij het afwijken van een deskundigenbericht namelijk hoge eisen aan de motivering.[204] Verkerk merkt terecht op dat het deskundigenbewijs hiermee snel een doorslaggevend bewijsmiddel wordt.[205]

In de praktijk is het overigens maar de vraag of de rechter in de hier bedoelde zaken snel zal overgaan tot het benoemen van een deskundige. In deze zaken hebben partijen immers zelf experts ingeschakeld van wie zij de verslagen in het geding brengen.[206] Het is ook denkbaar dat de rechthebbende wel maar de gedaagde geen expert heeft ingeschakeld maar enkel stelling heeft genomen door bijvoorbeeld te verwijzen naar relevante literatuur. In beide gevallen zal de rechter er eerder toe overgaan het bewijsmateriaal van partijen af te wegen dan om zelf weer een deskundige in te schakelen. Hij zal de afweging moeten maken tussen de noodzaak om een deskundige in te schakelen en de kosten en snelheid van een procedure. Het is daarbij ook de vraag of partijen zitten te wachten op de inzet van nog een deskundige die tijd nodig heeft voor (nog) een onderzoek. De rechter zal in de regel alleen een deskundige inschakelen wanneer de stellingen van partijen daar aanleiding toe geven, bijvoorbeeld omdat er fundamenteel verschil van mening blijft bestaan over een punt dat alleen door een deskundige kan worden opgehelderd.[207] Daarnaast kan nog gedacht worden aan de situatie die bijvoorbeeld in het merkenrecht voorkomt, waarin beide partijen een deskundigenverslag hebben ingebracht en waarbij beide partijen elkaars verslag betwisten. In die gevallen waarin ook partijen en rechters al vaker zijn geconfronteerd met specifieke deskundigenverslagen is het denkbaar dat hetzij de rechter zelf een notitie opstelt voor het inbrengen van een deskundigenverslag, hetzij partijen eventueel gezamenlijk om een door de rechter te

[201] Voorlopig verslag Tweede Kamer, zie Parl.Gesch. nieuw bewijsrecht, p. 316.
[202] Asser 2013, p. 228.
[203] Het deskundigenbericht is in die zin bijzonder dat het niet alleen als een bewijsmiddel (bijv. partij-rapportage) maar ook als een advies aan de rechter (deskundigenbericht ex art. 194 Rv) kan worden opgevat. Zie daarover o.m. De Bock 2011 (diss.), p. 298; HR 13 januari 1995, ECLI:NL:HR:1995:ZC1611, NJ 1997, 175, m.nt. CJHB, ov. 2.3.2 (De Heel/Korver): '(...) bewijs ook door een deskundigenbericht kan worden geleverd, en dat de waardering van het bewijs aan de rechter is overgelaten'.
[204] HR 5 december 2003, ECLI:NL:HR:2003:AN8478, JBPR 2004/29 m.nt. Schellaars (Nieuw Vredenburgh/Nieuwe Hollandse Lloyd), o.v. 3.6. Wanneer de rechter zienswijze van de deskundige volgt dan zal hij zijn beslissing in het algemeen niet verder behoeven te motiveren dan door aan te geven dat de door deze deskundige gebezigde motivering hem overtuigend voorkomt. Op specifieke en voldoende gemotiveerde bezwaren van partijen zal de rechter wel moeten ingaan. Wanneer de rechter de deskundige niet volgt (en partijen voldoende betwisten) dan, dient hij zijn oordeel zodanig te motiveren dat het mogelijk wordt zijn gedachtegang controleerbaar en aanvaardbaar te maken voor zowel partijen als derden.
[205] Verkerk 2007, p. 500. Visser (2008, p. 1992) laat in een onderzoek onder IE-rechters zien dat dit duidelijk anders is bij onderzoeken van partijdeskundigen. Daarin gaven rechters aan weinig belang te hechten aan door partijen ingebrachte deskundigenverklaringen en publiekonderzoeken vanwege het gebrek aan betrouwbaarheid en daardoor 'altijd achterdochtig' te zijn. De ervaring van rechters met beide was negatief.
[206] Zie bijvoorbeeld Hof Den Haag 29 oktober 2013, ECLI:NL:GHDHA:2013:3941; Rb. Arnhem 3 maart 2005, ECLI:NL:RBARN:2005:AS8529.
[207] Zie o.m. Schwartenberg 2013, p. 179.

benoemen deskundige verzoeken.[208] Doorgaans zal het in zaken waarin watermerken een rol spelen, blijven bij de inbreng van de partijdeskundigenverslagen. Voor het waarderen van watermerken en de inhoud van de deskundigenverslagen verwijs ik naar hoofdstuk 6.

4.2.4 Tussenconclusie

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te beoordelen is het watermerk in de context van het Nederlands civiele bewijsrecht geplaatst. De effectiviteit van bewijsmiddelen wordt daar beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en de stellingen die over dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd.

Als uitgangpunt van het Nederlandse civiele bewijsrecht geldt dat het aan partijen is overgelaten om door middel van onderbouwde stellingen de omvang en inhoud van het geschil te bepalen. Het is uiteindelijk aan de rechter overgelaten om het feit al dan niet vast te stellen. Om tot een beslissing te kunnen komen heeft de wetgever een stelsel in het leven geroepen waarin duidelijk wordt wie het bewijsrisico draagt wanneer het feit niet komt vast te staan.

In dit stelsel draagt de rechthebbende de bewijslast ten aanzien van het door hem te stellen feit dat het bestand aan de licentienemer toebehoort. Hij zal onder meer op grond van de mededelingsplicht het watermerk in de vorm van een rapportage direct bij de stukken aanvoeren ter onderbouwing van zijn stelling. Om te voorkomen dat de rechter dit feit direct vaststelt zal de gedaagde (licentienemer) dit feit gemotiveerd moeten betwisten. De rechthebbende zal daartoe in zijn rapportage voldoende aanknopingspunten moeten bieden aan de licentienemer. De gedaagde heeft bij gebrek aan medewerking en eventueel met de hulp van de rechter voldoende middelen om bewijs aan te voeren dan wel een contra-expertise uit te (laten) voeren.

De gedaagde kan ten aanzien van het watermerk in het licht van het gestelde feit in beginsel drie verweren voeren. De eerste twee verweren zien op het betwisten van de toelaatbaarheid en betrouwbaarheid van het watermerk. Beide verweren raken direct de effectiviteit van het watermerk dat er in bestaat dat het gestelde feit kan worden vastgesteld. Het derde verweer ziet op het gestelde feit. Ten aanzien van het gestelde feit kan de gedaagde de positie innemen dat er andere of alternatieve verklaringen bestaan dan dat hij het bestand openbaar heeft gemaakt. De gedaagde kan er bijvoorbeeld op wijzen dat iemand anders het bestand op

[208] Zie de Korte notitie Rechtbank Arnhem, sector civiel, december 2009: Benoeming deskundige in merken- en reclamezaken. Reglement voor versneld procederen in merken- en reclamezaken in de Rb. Arnhem. IEF 8436. En verder o.m. het tussenvonnis Rb. Arnhem, 9 september 2009, ECLI:NL:RBARN:2009:BJ8844 (Coca-Cola/ Superunie), ov. 4.1; Rb. ’s-Gravenhage, 25 november 2009, IER 2010, 10 (G-Star/Pepsi Raw II), ov. 4.26; Rb. ‘s-Gravenhage 11 mei 2011, IEF 9655 zaak HA ZA 09-414 (G-STAR/Pepsico), ov. 2.28. waarin partijen gezamenlijk een deskundige voorstellen en het eens worden over de opzet van het onderzoek. Rb. Gelderland 2 oktober 2013, ECLI:NL:RBGEL:2013:6444 (Jager/Jager), ov. 2.2 acht zich vrij zelf een deskundige aan te wijzen nu partijen zelf niet tot een eensluidend voorstel zijn gekomen tot aanwijzing van een deskundige.

internet heeft geplaatst. Dit laatste verweer raakt de effectiviteit van het watermerk niet. De rechter kan de door de rechthebbende aangevoerde stelling dat het bestand aan de gedaagde toebehoort immers vaststellen. De gedaagde betwist niet de door het watermerk te bewijzen stelling dat het bestand aan hem toebehoort, maar betwist hier het verband tussen het op internet aangetroffen bestand en zijn schuld. Het is immers aan de rechthebbende om te stellen en zo nodig te bewijzen dat zijn werk openbaar is gemaakt door de gedaagde. Zonder die vaststelling is er geen sprake van inbreuk op het auteursrecht. Voor een succesvol verweer dient de gedaagde zijn stelling dat er sprake is van een alternatieve verklaring wel te onderbouwen. De rechthebbende zal in dat geval wijzen op een zorgplicht voor de gedaagde om de content te beschermen. Het is daarmee niet onmogelijk, maar ook niet eenvoudig om een alternatief verweer te voeren voor de stelling dat het bestand aan de licentienemer toebehoort en dat het aan hem te wijten is dat het onrechtmatig bestand op internet is geplaatst.

Wanneer de rechter van oordeel is dat partijen voldoende hebben gesteld en betwist kan de rechter het feit voorshands aannemen en de wederpartij toelaten tot het leveren van tegenbewijs. Hij kan de rechthebbende ook een bewijsopdracht geven ten aanzien van het gestelde feit. De rechter kan ook een deskundigenbericht vragen wanneer hij graag meer informatie zou willen over een punt waarover partijen nog van mening verschillen. Partijen kunnen daarop reageren. Tot slot geeft de rechter een definitief bewijsoordeel dat in dialoog met partijen tot stand is gekomen. De bewijsbeslissing is daarmee tot stand gekomen binnen de ruimte die de stellingen van partijen hebben gelaten.

De rechter is bij gebrek aan wettelijke bepalingen ten aanzien van de waardering van watermerken vrij in de waardering ervan. Ook in de (buitenlandse) jurisprudentie zal de rechter geen steun vinden voor de waardering van watermerken. Het komt ervoor de rechter dan op aan om zelf tot een oordeel te komen eventueel met de hulp van een door hem zelf benoemde deskundige dan wel op basis van de door partijen ingebrachte verslagen, experts of andere materialen. In de praktijk zal de rechter zijn beslissing veelal beoordelen in het licht van hetgeen partijen hebben ingebracht.

4.3 Beslissen over feiten naar Belgisch civiel recht

Als uitgangspunt geldt ook in het Belgisch civiele recht dat het aan partijen is overgelaten om stellingen aan te dragen, te onderbouwen en daarmee de omvang en inhoud van het geschil te bepalen. [209] De partijwerkzaamheid neemt in België dan ook een voorname rol in de literatuur in.[210] De rechter is in beginsel lijdelijk maar heeft wel een duidelijk initiatiefrecht om in het kader van de juridische waarheidsvinding het nodige bewijs te verzamelen.[211] Hij heeft

[209] Zie o.m. Cattoir 2013, p. 29, 34, 49; Allemeersch 2007 (diss.), p. 67.
[210] In de Belgische literatuur lijkt de partijwerkzaamheid in het bewijsrecht een nadrukkelijkere rol te spelen dan in de Nederlandse literatuur.
[211] Zie o.m. Cattoir 2013, p. 31, 50 en meer uitgebreid p. 116; Laenens e.a. 2012, p. 535; Allemeersch 2007 (diss.), p. 349. Zo heeft ook de rechter in België de mogelijkheid om bijkomende vragen te stellen tijdens de

daartoe ook de nodige onderzoeksmaatregelen ter beschikking gekregen maar zal zich wel moeten laten leiden door de proceseconomie (art. 875bis Ger. W.).[212] Daarbij zal hij steeds voor ogen moeten houden dat het civiele proces bij uitstek door de partijen wordt begrensd.[213] Het is uiteindelijk zijn taak om het geschil te beslechten en in casu om te beslissen of het gestelde feit kan worden vastgesteld.[214] Laenens en anderen merken op dat de taak van de civiele rechter inzake bewijsvoering aanzienlijk evolueert en deze van de strafrechter zelfs in sterke mate evenaart ondanks dat de bewijsregelingen sterk verschillen.[215]

Om de procedure zo redelijk en efficiënt mogelijk te laten verlopen moeten ook in België partijen de rechter en elkaar zoveel en zo vroeg mogelijk in de procedure duidelijkheid verschaffen over het geschil.[216] Op beide partijen rust vanuit de beginselen van procesloyauteit en proceseconomie dan ook een medewerkingsplicht waaronder een informatie en mededelingsplicht.[217]

Iedere partij moet bewijs leveren van de feiten die zij aanvoert waarmee bewijslastverdeling als hoofdregel gegeven is.[218] Bij aanvang van de procedure is het evenals naar Nederlands recht aan de rechthebbende om de feiten aan te voeren waarop hij zijn aanspraak baseert. De rechthebbende (eiser) hoeft het feit dat het bestand aan de licentienemer toebehoort alleen te bewijzen wanneer de licentienemer (wederpartij) het feit heeft betwist. Uiteindelijk is het aan de rechter om te beoordelen of het gestelde feit dat het bestand aan de licentienemer toebehoort kan worden vastgesteld. Het watermerk is dan effectief wanneer de rechter dat feit bewezen kan achten.

Om de vraag naar de bewijswaarde van het watermerk in België te kunnen beantwoorden moet eerst het watermerk gekwalificeerd worden als bewijsmiddel. Het Burgerlijk Wetboek bevat een numerus clausus aan bewijsmiddelen. Dit gesloten stelsel van bewijs geldt alleen voor het bewijs van rechtshandelingen en niet voor het bewijs van feiten.[219] De rechter is dan vrij om dat vermoeden al dan niet aan te nemen op basis van de rapportage van de rechthebbende en de verweren van de gedaagde.

---

zitting (art. 756ter Ger.W.) en na het sluiten van de debatten ook door een ambtshalve heropening ervan (art. 774 Ger.W.).

[212] Laenens e.a. 2012, p. 535.

[213] Van Reepinghen, Verslag over de Gerechtelijk Hervorming, BS 1964, 266. Zie voor de ontwikkelingen Allemeersch 2007, p. 671.

[214] In België geldt in burgerlijke zaken een bij wet gereglementeerd stelsel van bewijs, terwijl in handelszaken het bewijs in principe vrij is. De toepasselijke bewijsregels worden bepaald door de aard van het geschil. Zoals in de inleiding reeds omschreven beperkt zich verder tot bewijs in burgerlijke zaken.

[215] Laenens e.a. 2012, p. 535.

[216] Zie meer rechtsvergelijkend perspectief ook Verkerk 2010 (diss.), p. 376.

[217] Art. 871 en 877 Ger. Wetboek. Zie verder o.m; Cattoir 2013, p. 33.

[218] Art. 870 Ger. W.; art. 1315 BW Voor de verschillen tussen beide bepalingen zie o.m. Cattoir 2013, p. 69. Laenens e.a. 2012, p. 537; Allemeersch 2007 (diss.) p. 353 en de daar aangehaalde literatuur;

[219] Dit behoudens de gevallen waarin de wederpartij de feiten erkent. In die gevallen is er een bekentenis en is geen watermerk meer nodig. Zie voor het gesloten stelsel verder par. 5.2.1.2.

Het bewijsrecht in burgerlijke zaken is gereglementeerd ten aanzien van de toelating van de bewijsmiddelen, hun bewijskracht en hun onderlinge hiërarchie.[220] Dit geldt zowel voor bewijs ten aanzien van rechtshandelingen als voor het bewijs van materiële feiten en rechtsfeiten. Ten aanzien van deze laatste categorie is de reglementering echter minder verstrekkend omdat in de regel de in de wet toegekende bewijswaarde alleen toepassing vindt wanneer zij de rechter al dan niet overtuigt van het bestaan van de feiten waarvoor zij als bewijs dient. Dit heeft tot gevolg dat bij het bewijs van deze feiten het feitelijk vermoeden de vooraanstaande rol inneemt die het schriftelijk bewijs bij rechtshandelingen vervult.[221] De bewijsvoering bij feiten is dan in zoverre minder gereglementeerd, omdat men in de regel terugvalt op feitelijke vermoedens en/of deskundigenonderzoeken, waarbij de bewijswaarde vrij is. De beperking van de rechterlijke vrijheid ten aanzien van de toelating van het bewijs wordt in de literatuur ook wel als log, complex en onrechtvaardig gezien.[222] Toch wordt er ook op het doel gewezen dat het de snelheid zou bevorderen en in een eenvoudige procedure wel meer rechtszekerheid biedt.[223] In de praktijk ontstaat er bijvoorbeeld door de medewerkingsplicht van partijen (en soms derden) wel ruimte met betrekking tot de in beginsel strakke regels.[224]

Hoewel de gronden waarop de rechter in België tot de vaststelling van feiten mag komen uiteindelijk niet verschilt met Nederland, kennen zij behoudens de waardering door de rechter zelf, in beide landen een andere grondslag. Zo is het vaststellen van feiten op grond van algemene bekendheid en ervaringsregels alsmede de erkenning en niet-betwisting niet bij wet geregeld. In België wordt de bron gevonden in de rechtspraak en literatuur.[225] De uitdrukkelijke erkenning (i.e. gerechtelijke bekentenis) is wel bij wet geregeld.[226] Het gebrek aan wettelijke grondslag en daarmee een duidelijke keuze laat zich het beste zien ten aanzien van het 'niet-betwisten' van feiten.[227] Deze wordt veelal benaderd als een variant van erkenning in de vorm van een stilzwijgende erkenning. Het centrale probleem wordt dan gevormd door de wil of intentie van partijen. Een louter gebrek aan betwisting lijkt niet voldoende daar de betekenis van erkenning aan toe te kennen. In de praktijk grijpt de rechter dan ook wel terug naar het feitelijk vermoeden (art. 1353 BW) om een feit vast te stellen als niet aan de voorwaarden voor erkenning kan worden voldaan. In de literatuur verschillen de meningen over de te volgen weg van het vermoeden of de procesrechtelijke benadering die

[220] Zie o.m. Cattoir 2013, p. 134; Laenens e.a. 2012, p. 531; Wagner 2009, p. 153; Allemeersch 2007 (diss.), p. 345. Bewijswaarde en bewijskracht zijn in België zowel in de rechtspraak als literatuur vrij eng omschreven begrippen. Bewijswaarde is de mate waarin de rechter, afhankelijk van de wettelijke regeling, een bewijsmiddel als overtuigend moet of mag beschouwen. Bewijskracht wijst op de inhoud van geschreven documenten. Een rechter die hiervan afwijkt schendt de bewijskracht van die overeenkomst.
[221] Cattoir 2013, p. 145. Cattoir merkt ook op dat het onderscheid tussen rechtshandelingen en de hier bedoelde feiten niet altijd absoluut te maken is.
[222] Zie o.m. Cattoir 2013, p. 24 en de daar aangehaalde literatuur; Laenens e.a. 2012, p. 536.
[223] Zie o.m. Cattoir 2013, p. 23 en de daar aangehaalde literatuur.
[224] Laenes 2004, p. 273 en 288.
[225] Zie o.m. Cattoir 2013, p. 59-62. Allemeersch 2007 (diss.), p. 333 en 383, Storme 1962, p. 290 en de daar aangehaalde literatuur.
[226] Zie de artt. 1354-1356 BW.
[227] Zie Allemeersch 2007 (diss.), p. 389 voor de ontwikkelingen en verschillende standpunten in literatuur en rechtspraak tot 2007.

vanuit de partijwerkzaamheid tot de conclusie komt dat een onvoldoende gemotiveerde betwisting gelijk kan worden gesteld met een stilzwijgende erkenning.[228] Wanneer de gedaagde het feit erkent zal het watermerk verder geen rol meer spelen in de procedure. In de regel geldt hetzelfde als de gedaagde het feit niet betwist omdat in beide benaderingen de rechter het feit uiteindelijk zal vaststellen. In deze paragraaf zal de nadruk liggen op de situatie waarin de gedaagde het gestelde feit, dat het bestand aan hem toebehoort, betwist. Wanneer de gedaagde het feit erkent zal het watermerk ook in België immers geen rol meer spelen in de procedure.

De effectiviteit van watermerken wordt ook naar Belgisch civiel bewijsrecht beoordeeld in het licht van de door rechthebbende te bewijzen stelling dat het bestand aan de licentienemer toebehoort, en welke stellingen over dat feit en het watermerk zijn aangevoerd.

Vanuit dit perspectief wordt ook vanuit Belgisch recht aandacht besteed aan de vraag welke stellingen partijen moeten en redelijkerwijs kunnen aanvoeren over watermerken en op welke wijze de rechter deze stellingen moet beoordelen. Om die reden wordt eerst ingegaan op de bewijsrisicoverdeling (par. 4.4.1). Daarbij zal nader worden ingegaan op de vraag welke stellingen partijen dienen aan te voeren en welke mogelijkheden de rechter heeft om feiten vast te stellen en via de bewijslastverdeling het vaststellen van feiten zo eerlijk en efficiënt mogelijk te laten verlopen. Daarna wordt ingegaan op aannemelijke verweren die de gedaagde (licentienemer) kan aanvoeren om het watermerk ineffectief te maken (par. 4.4.2). Tot slot wordt gekeken naar vraag hoe de rechter tot zijn bewijsoordeel komt (par. 4.4.3). De paragraaf wordt afgesloten met de tussenconclusie (par. 4.4.4).

4.3.1 Bewijsrisicoverdeling

Om de rechter de mogelijkheid te geven om uiteindelijk tot een beslissing te komen heeft de wetgever ervoor gekozen om het risico dat de gestelde feiten in een procedure onduidelijk blijven toe te delen aan de partij die de bewijslast voor dat feit draagt.[229] Vervolgens is in de rechtspraak inmiddels uitgebreide jurisprudentie ontwikkeld ten aanzien van de bewijsrisico-verdeling.
Een procedure verloopt in België in beginsel niet veel anders dan in Nederland. Ook in België is het aan partijen om stellingen aan te voeren en deze stellingen te onderbouwen door middel van bewijsstukken. Het voornaamste verschil tussen beide landen is gelegen in het feit dat in België geen formeel stelsel van bewijsaanbod en bewijsopdracht bestaat.

[228] Cattoir 2013, p. 62. Allemeersch 2007 (diss.), p. 394 merkt op dat in Nederland, Duitsland, Zwitserland en Spanje de wetgever de voorkeur heeft gegeven aan de procesrechtelijke benadering. Het Hof van Cassatie bevestigde deze lijn in 2008 door arrest te wijzen dat enkel de betwiste feiten moeten worden bewezen. Cass. 18 april 2008, C.07.0409.F; Cass., 10 mei 2001, AR C.99.0355.F, A.C. 2001, 270.
[229] Zie voor achtergronden van de bewijsrisicoverderling o.m. Cattoir 2013, p. 39; Allemeersch 2007 (diss.), p. 353.

In vergelijking met Nederland kan de wijze waarop de rechter in België tot het vaststellen van feiten komt in twee fasen worden onderverdeeld omdat in België zoals gezegd geen fase bestaat van bewijsaanbod en bewijsopdracht. In het navolgende worden de twee fasen nader uitgewerkt.[230] De eerste fase ziet op het stellen en betwisten van stellingen door partijen (par. 4.3.1.1). Het is in deze fase aan de rechter om te oordelen of partijen voldoende hebben gesteld dan wel betwist. Indien hij tot dat oordeel komt zal de rechter in de volgende fase de bewijslastverdeling moeten vaststellen om te bepalen welke partij als eerste tot het leveren van bewijs wordt toegelaten (par. 4.3.1.2)

4.3.1.1 Aanvoeringsrechten en -plichten

Evenals in Nederland draagt de partij die het beoogde rechtsgevolg inroept de aanvoeringslast, libelleringslast of charge d'allégation.[231] Dit geldt zowel voor de vordering van de eiser als voor het zelfstandig verweer van de gedaagde. Ook naar Belgisch recht zal de aanvoeringslast bij de rechthebbende liggen alsmede het bewijsrisico dat wanneer hij er niet in slaagt zijn stelling te bewijzen, het feit niet door de rechter zal worden vastgesteld.

De eiser die zijn subjectief recht wil afdwingen zal ten eerste de feiten moeten aanvoeren die het mogelijk maken om alle voorwaarden te vervullen die nodig zijn voor de toepassing van de rechtsregel.[232] Evenals naar Nederlands recht zal hij feiten moeten aanvoeren die bewijzen dat de licentienemer inbreuk heeft gemaakt op het auteursrecht. Ook in België zal voldoende moeten worden aangevoerd om te voorkomen dat de vordering wordt afgewezen wegens aanvoering van onvoldoende feiten.

Beide partijen dragen op grond van de medewerkingsplicht verantwoording voor het aanbrengen van de feiten.[233] Het is dan ook niet zo dat de gedaagde in het licht van bewijsrisicoverdeling kan afwachten of de eiser slaagt in het bewijzen van de door hem gestelde feiten. In de literatuur is er ook op gewezen dat het ook niet in het voordeel van de gedaagde zou werken om af te wachten. Het is immers moeilijker de overtuiging van de rechter te weerleggen dan te voorkomen dat deze zich ontwikkelt.[234] In vergelijking met Nederland is het in de praktijk bij aanvang van het geding niet altijd duidelijk wie wat moet bewijzen.[235] Bij de verdeling van de bewijslast zoekt de rechter vaak een pragmatische oplossing waarbij de aard van het geschil en de toepasselijke materiële regels een rol kunnen spelen.[236] De formele uitwisselingen van bewijsaanbod en bewijsopdracht zijn grotendeels verdwenen in het Gerechtelijk Wetboek van 1967. Partijen mogen sindsdien bewijs leveren

[230] Zie voor andere mogelijk indelingen ook Cattoir 2013 en Allemeersch 2007 (diss.)..
[231] Allemeersch 2007 (diss.), p. 121; Bosse 2003 (diss.), p. 13.
[232] Cattoir 2013, p. 55;
[233] Zie o.m. de meewerkingsplicht van art. 877 Ger.W.; Zie uitgebreid Allemeersch 2007 (diss.), p. 442 voor sancties op medewerking.
[234] Zie o.m. Mougenot 2002, p. 93: 'Il sait qu'il est plus habile d'empêcher une conviction de se former que de renverser une conviction qui a déjà pris corps'; Cattoir 2013, p. 78.
[235] Zie ook Bosse 2003 (diss.), p. 25.
[236] Bosse 2003 (diss.), p. 25.

wanneer zij willen. In een eenvoudig verzoek in hun conclusies kunnen zij, indien zij dit wensen ook een onderzoeksmaatregel vragen, zoals de inzet van een deskundige.[237] Hiermee is tevens meer vrijheid gegeven aan de rechter omdat deze zich niet langer gebonden ziet aan de formules van het bewijsaanbod en de antwoorden daarop.[238] In vergelijking met Nederland is de Belgische bewijsregeling dan ook minder formeel van aard dan het Nederlandse stelsel van bewijsaanbod en bewijsopdracht.[239] De Nederlandse benadering heeft als voordeel dat partijen duidelijk weten wat ze (nog) moeten bewijzen en waar ze aan toe zijn.

In de praktijk brengt iedere partij direct de bewijzen van haar stellingen naar voren. De rechthebbende zal ook in België het watermerk reeds bij de stukken (na de conclusie) aanvoeren. Evenals in Nederland geldt dat wanneer de rechthebbende een zorgvuldig verslag bij zijn stukken voegt, hij de drempel van het bewijs voor de wederpartij verhoogt. Wanneer de rechthebbende het watermerk in de vorm van een uitgebreide rapportage als bewijsmiddel inbrengt dan kan de gedaagde niet langer volstaan met een eenvoudige ontkenning om te voorkomen dat de rechter tot de overtuiging komt dat het bewijsmiddel betrouwbaar is en op grond daarvan het feit vaststelt. In het licht van het aanbrengen van bewijs zal de gedaagde er in de praktijk verstandig aan doen om ook een expert in te schakelen voor het leveren van een eigen (partij-)deskundige(verslag) bijvoorbeeld ten aanzien van gevolgde methodologie of gebruikte technieken.

Nadat partijen hun stellingen hebben aangevoerd en zonodig bewezen bekijkt de rechter vervolgens het dossier en beoordeelt daarin zelf het betoog van partijen.[240] Wanneer de rechter de gestelde feiten voldoende bewezen acht dan zal hij deze vaststellen. De verdeling van de bewijslast of beter gezegd het bewijsrisico is evenals in Nederland vooral van belang wanneer de feiten niet duidelijk zijn geworden voor de rechter.

De rol van de rechter is in theorie anders dan in Nederland. Allemeersch merkt in navolging van Taruffo op dat rechters in België en Frankrijk het grootste arsenaal aan ambtshalve te bevelen onderzoeksmaatregelen kennen.[241] Hij merkt tegelijk op dat veel Belgische rechters door een hoge werkdruk de ingereedheidbrenging afwachten alvorens het dossier grondig te bestuderen waardoor hij in de praktijk deze bevoegdheden nauwelijks in de praktijk kan brengen en ervoor zal kiezen om de initiatieven van partijen af te wachten.[242] De rechter in Nederland bestudeert ook in de praktijk het dossier en heeft in tegenstelling tot zijn Belgische

[237] Allemeersch (2007 (diss.), p. 347) beschrijft vanaf deze pagina tevens het gehele proces van deformalisering.
[238] Allemeersch 2007 (diss.), p. 347.
[239] Zie daarover Allemeersch 2007 (diss.), p. 365. België kende tot de herziening van het Gerechtelijk Wetboek van 1967 ook een stelsel van bewijsaanbod en bewijsopdracht. Zie Allemeersch die dit proces beschrijft op p. 347.
[240] Het is de rechter ook toegestaan om zijn beslissing te baseren op feiten die blijken uit de stukken maar niet door partijen zijn ingeroepen. Zie o.m. Cass. 12 november 1987, RW 1987-88, 1379, m.nt. J.L.; Cass. 11 maart 2002, Pas. 2002, I, 690; Cattoir 2013, 50.
[241] Allemeersch 2007 (diss.), p. 364 onder verwijzing naar Taruffo, 'rethinking the standaards of proof, american ournal of compartive law 2003 , p. 659.
[242] Allemeersch 2007 (diss.), p. 365.

collega meer mogelijkheden (ter comparitie) de bewijsgaring te sturen. In België heeft de rechter minder mogelijkheden om het debat van partijen te sturen. De Nederlandse rechter kan hierdoor sneller tussen partijen komen en het proces de juiste richting opsturen. Iets wat volgens Allemeersch de (juridische) waarheidsvinding ongetwijfeld ten goede komt.[243]

Anders gezegd partijen brengen een argumentatielijn ondersteund met bewijzen in en de rechter zal deze vooral in consistentie nalopen. De rechter zal aan de hand van beide verhalen nagaan welke feiten in beide verhalen overeenkomen en dus voor waar kunnen worden aangenomen. Het komt dan evenals in de Nederlandse procedure aan op punten waar de verhalen uiteenlopen. De rechter zal daar een oordeel over moeten vellen. Wanneer de effectiviteit van het watermerk als juridisch bewijsmiddel centraal komt te staan dan gaat het er ook naar Belgisch recht in wezen om dat het watermerk in staat is om het gestelde feit te bewijzen. Een betrouwbaar watermerk leidt zonder meer tot de conclusie dat het bestand aan de gedaagde toebehoort. Ook wanneer de gedaagde er onvoldoende in slaagt het watermerk als bewijs te weerleggen en ook de rechter geen aanleiding ziet om de betrouwbaarheid van het watermerk verder ter discussie te stellen dan staat het feit vast. Daarmee is het watermerk in de context van het bewijsrecht evenals naar Nederlands recht het geval is een effectief bewijsmiddel zonder dat de betrouwbaarheid zelf (voldoende) getoetst is.

Evenals naar Nederlands recht geldt in België dat de rechter zijn beslissing mag baseren op het gegeven dat de wederpartij het feit niet heeft betwist. Hoewel deze regel eerder door het Hof van Cassatie nog open was geformuleerd door aan te nemen dat de rechter die zijn beslissing grondt op de beweringen van een procespartij die door de tegenpartij niet worden betwist, de regel inzake de objectieve bewijslast niet schendt, formuleert het Hof deze thans in overeenstemming met de feitenrechtspraak en de literatuur.[244] Dat betekent dat de rechter de aangevoerde feiten kan vaststellen als deze niet worden betwist. Er is sprake van niet-betwisten wanneer de verwerende partij het door de eisende partij aangevoerde feit erkent, uitdrukkelijk niet betwist of zich daar niet over uitspreekt. Wanneer de verwerende partij het feit erkent dan hoeft dat feit niet langer te worden bewezen.[245] Als de verwerende partij het feit uitdrukkelijk of stilzwijgend niet-betwist ontstaat er een andere situatie. In beginsel geldt daarvoor dat de eisende partij van haar bewijslast is bevrijd zolang de verwerende partij het niet herroept. Dit leidt ook uitzondering wanneer uit de wet of bijzondere omstandigheden blijkt dat er sprake is van een erkenning.[246] Voor de betwisting van het feit volstaat het in beginsel dat de verwerende partij het aangevoerde feit eenvoudig ontkent.[247] Vanzelfsprekend betwist hij het ook wanneer hij andere feiten aanvoert die bewijs vereisen.

[243] Allemeersch 2007 (diss.), p. 365.
[244] Cass. 25 oktober 1979, A.C. 1979-80, 261; Cass. 10 mei 2001, Pas. 2001, I, 807; Zie voor de ontwikkelingen en verschillende standpunten in literatuur en rechtspraak tot 2007 Allemeersch 2007 (diss.), p. 389; Voor ontwikkelingen daarna o.m. Wagner 2009, p. 162; Cattoir 2013, p. 62 en de daar aangehaalde literatuur.
[245] Zie voor de erkening als bekentenis ook de artt. 1354-1356 BW en o.m. Samyn 2012, p. 106.
[246] Cass. 2 december 1971, Pas. 1972, I, 323; Cass. 26 september 1991, A.C. 1991-92, 97; zie ook Cattoir 2013, p. 65; Samyn 2012, p. 131.
[247] Samyn 2010, p. 57.

Evenals naar Nederlands recht speelt ook in België de dynamiek in het partijdebat een belangrijke rol. Het geschil kan door partijen tot enkele twistpunten worden beperkt wanneer met name de verwerende partij de feiten erkent dan wel betwist. Wanneer de verwerende partij geen verweer voert vereenvoudigt hij de objectieve bewijslast van de eiser. Hij neemt daarmee een risico de procedure te verliezen.[248] Dat verschilt in zoverre met de situatie in Nederland dat de procedure in Nederland in de eerste fase al kan eindigen vanwege een onvoldoende betwisting. Cattoir merkt op dat in België een passieve houding nog kan lonen, al houdt zij altijd een risico in.[249] Dat is anders dan in Nederland waar een passieve houding hetzelfde risico inhoudt maar de rechter in de praktijk veel zaken beslecht door aan te nemen dat een feit onvoldoende is betwist waardoor de gedaagde dat feit en mogelijk de procedure verliest.

Cattoir merkt op dat de bewijsvoering in werkelijkheid niet volgens de strakke structuur van 870 Ger. W. en 1315 BW loopt. De verweerder zal vanaf het begin feiten aanvoeren ter onderbouwing van zijn standpunt.[250]

4.3.1.2 Bewijslastverdeling

Evenals naar Nederlands recht is de verdeling van de bewijslast vooral van belang als het gepresenteerde bewijs niet heeft overtuigd.[251] Voor de verdeling van de bewijslast wordt ook wel onderscheid gemaakt tussen de subjectieve en objectieve bewijslast. De subjectieve bewijslast ziet kort gezegd op de vraag wie moet bewijzen en verwijst naar de last die er bestaat om het bewijs aan te brengen. De objectieve bewijslast ziet kort gezegd op de vraag wat moet worden bewezen en wijst op het risico om het proces te verliezen wanneer onvoldoende bewijs is geleverd. Ook in België wordt dan gesproken over bewijsrisico.[252]

De kern van de bewijslastverdeling is in België neergelegd in artikel 870 Ger. W. waarin is opgenomen dat iedere partij het bewijs moet leveren van de feiten die zij aanvoert.[253] Dit artikel vat samen wat al eerder in artikel 1315 BW was opgenomen namelijk dat degene die de uitvoering van een verbintenis vordert het bestaan daarvan moet bewijzen.[254] Degene die beweert bevrijd te zijn van de uitvoering van deze verbintenis moet het bewijs leveren van de betaling of van het feit dat het tenietgaan van zijn verbintenis heeft teweeggebracht. Deze bepaling is toepasselijk op het bewijs van alle feiten die rechtsgevolgen met zich mee kunnen brengen.[255]

[248] Zie o.m. Cattoir 2013, p. 67.
[249] Cattoir 2013, p. 65.
[250] Zoals eerder gesteld is het immers eenvoudiger te verhinderen dat een overtuiging ontstaat dan een reeds gevormde overtuiging om te buigen. Zie o.m. Cattoir 2013, p. 78; Mougenot 2002, p. 93.
[251] Zie ook Bosse 2003 (diss.), p. 25.
[252] Cass. 17 september 1999, A.C. 1999, 1119; Allemeersch 2007 (diss.) p. 353.
[253] Zie o.m. Cattoir 2013, p. 70.
[254] Allemeersch 2007 (diss.), p. 353.
[255] Storme 1962, p. 89; Voor de verschillen kan verwezen worden naar Storme 1990, TPR 1990, 353, p. 505; Allemeersch 2007 (diss.), p. 353; Cattoir 2013, p. 70.

De later in artikel 870 Ger. W. gekozen formulering wordt in de literatuur als ongelukkig ervaren omdat ze ten onrechte enkel verwijst naar feiten terwijl ook bewijs van rechtshandelingen moeten worden geleverd en het artikel ten onrechte de indruk wekt dat de aanvoeringslast samenvalt met de bewijslast.[256] De regel van 1315 BW en 870 Ger. W. is volgens Laenens ook niet absoluut te noemen omdat steeds meer wordt aangenomen dat de bewijslast in civiele zaken niet alleen mag afhangen van de toevallige processuele positie als eiser of verweerder.[257]

Het uitgangspunt is ook in België dat de partij die zich beroept op de rechtsgevolgen van bepaalde rechtsfeiten of rechten de bewijslast daarvan draagt en omgekeerd dat de partij die beweert bevrijd te zijn van een bepaalde verplichting het bewijs daarvan levert. De bewijslast blijft echter in beginsel bij de partij die de rechtsgevolgen inroept, in casu de rechthebbende. De inhoud van de bewijslast wordt evenals in Nederland mede bepaald door de inhoud van het materieel recht.[258] Evenals naar Nederlands recht zal het in voorkomend geval ook naar Belgisch recht aan de rechthebbende zijn om als eiser de inbreuk op het auteursrecht te bewijzen. Zoals eerder opgemerkt betekent dit niet dat gedaagde achterover kan leunen. Via het principe van procesloyauteit is algemeen erkend dat er een medewerkingsplicht bestaat tussen partijen.[259] Het proces is geconditioneerd door de fair play die de procespartijen hebben tegenover elkaar en de plicht die ze hebben inzake de bewijsvoering.[260] Er wordt ook wel gesproken van partijwerkzaamheid, hetgeen inhoudt dat partijen een proces voeren in het licht van een goede procesorde en proceseconomie.[261] Dat brengt met zich mee dat de partij die het bewijsrisico draagt ook medewerking van de verweerder mag verwachten in die zin dat hij niet belet wordt het bewijs te verzamelen dat hij nodig heeft. Doordat de bewijslast geen verplichting inhoudt maar een risico staat niets er aan in de weg dat de rechter zich ook mag inspannen om het bewijs boven tafel te krijgen.[262]

Om te voorkomen dat de rechter tot de overtuiging komt dat het gestelde juist is zal de gedaagde het gestelde feit voldoende moeten betwisten. Vanuit de gedachte van waarheidsvinding en procesloyauteit zal hij duidelijk moeten maken hoe de feiten volgens hem in elkaar zitten.[263] Wat en hoeveel hij moet bewijzen hangt ook af van de bewijzen die de wederpartij aan zijn stelling ten grondslag heeft gelegd. Zo gelden de regels van de bewijslastverdeling ook ten aanzien van negatieve of complexe feiten waarvan het veel

[256] Zie Storme 1990, p. 505; Laenens 2004, p. 277.
[257] Laenens 2004, p. 277. Voor de verschillen tussen beide bepalingen zie Allemeersch 2007 (diss.) p. 353 en de daar aangehaalde literatuur; Laenens e.a. 2012, p. 537; Cattoir 2013, p. 70.
[258] In casu betreft het een casus naar auteursrecht. Zie daarvoor par. 3.4.
[259] Zie voor de stelregel dat partijen loyaal moeten samenwerken aan een goede bewijsvoering o.m. art. 877 Ger. W.. Zie ook Allemeersch 2007 (diss.), p. 353.
[260] Laenens 2004, p. 278; Allemeersch 2007, p. 355.
[261] Allemeersch 2007, p. 396.
[262] Cass. 25 september 2000, A.C. 2000, 1424, P&B 2001, 114, m.nt. B. Allemeersch; Zie ook Allemeersch 2007 (diss.), p. 354 voor de historie.
[263] Storme 1990, p. 353; Allemeersch 2007 (diss.), p. 397.

moeilijker is om bewijs te leveren. In die gevallen kan de rechter het bewijs aannemen op basis van (een feitelijke vermoeden van) waarschijnlijkheid. Op de wederpartij rust dan de last om precieze feiten aan te voeren en te bewijzen waaruit het tegendeel blijkt.[264] Het Hof van Cassatie heeft er in die gevallen niet voor gekozen om de bewijslast om te keren.[265] De regel dat een partij zijn stelling ook moet bewijzen kan evenals naar Nederlands recht worden verzacht door het zogenoemde vermoeden.[266] Maar evenals naar Nederlands recht is er in België ook weinig reden om af te wijken van de hoofdregel dat in dit geval de rechthebbende de volledige bewijslast draagt.

Om de betwistingslast te kunnen handhaven mag de rechter hieraan het bewijsrisico verbinden dat wanneer een partij onvoldoende betwist het bewijsrisico bij die partij komt te liggen.[267] Het feit staat dan vast behoudens het bewijs van tegendeel.[268] De rechter hoeft dan geen verdere bewijsgaring te bevelen. De partijwerkzaamheid geeft de rechter de mogelijkheid om zaken te beoordelen in de omstandigheden van het geval.[269] Wanneer een feit wordt aangevoerd waarvan de wederpartij de waarheid onmogelijk kan achterhalen heeft de rechter de mogelijkheid om het feit niet als vaststaand te beschouwen terwijl hij het feit kan vaststellen wanneer hij van mening is dat de wederpartij dit wel eenvoudig kan beoordelen. Het feit staat dan vast zolang hij het niet expliciet heeft betwist.[270]

Het is ook in België niet ondenkbaar dat de gedaagde in bewijsnood kan komen omdat hij niet over alle gegevens beschikt. Dit is ook bij watermerken niet ondenkbaar, bijvoorbeeld omdat de rapportage onvolledig of onduidelijk is op bepaalde technische punten. De rechthebbende zal in de regel deze gegevens direct verstrekken vanwege zijn bewijspositie. Hoe beter onderbouwd zijn bewijs is, hoe sterker immers zijn stelling. Daarnaast zal de rechthebbende willen voorkomen dat de rechter ingrijpt door een bevel te geven het bewijs te overleggen.[271] Van belang is wel dat het stuk bestaat. De rechthebbende moet dus geen extra werk hoeven te verzetten om de gegevens te krijgen.[272] Ook in België kan voor die gevallen analoog aansluiting worden gezocht ten aanzien van zaken in het medisch aansprakelijkheidsrecht waarbij evenals in Nederland via de verzwaarde motiveringsplicht, onder voorwaarden wordt aanvaard dat de eiser, op wie de bewijslast rust, door de wederpartij in de gelegenheid moet worden gesteld om voldoende verweer te kunnen voeren. Evenals in Nederland is ook in België voor deze gevallen omkering van de bewijslast niet snel denkbaar.[273] Wel kan de

[264] Cattoir 2013, p. 76.
[265] Cass. 14 januari 2005, NJW 2005, 699, m.nt. E. Brems, RCJB 2006, m.nt J. Van Drooghenbroeck en S. Van Drooghenboeck.
[266] Cattoir 2013, p. 84. Vermoedens vormen een bewijsmiddel op grond waarvan de rechter tot zijn eindoordeel mag komen.
[267] Zie Allemeersch 2007 (diss.), p. 397.
[268] Naar Nederlands rechter wordt dan gesproken van de figuur van ‘voorhands aannemen’.
[269] Allemeersch 2007 (diss.), p. 397.
[270] Partijen mogen echter niet worden verrast doordat de rechter alsnog beslist dat het feit niet is komen vast te staan terwijl het feit niet is betwist, bijvoorbeeld door aandacht hiervoor te vragen in het debat.
[271] Art. 871, 877 Ger. W.; Cattoir 2013, p. 116. Vgl. de voorwaarden van art. 843a Rv in Nederland.
[272] Bergen 1 oktober 2002, JT 2002/815; Cattoir 2013, p. 117.
[273] Cass. 16 december 2004, AR C030407N

rechter in die gevallen aan de eiser minder strenge eisen aan het bewijs stellen van een negatief feit of een partij verplichten tot het overleggen van documenten.[274] Op het niet meewerken kunnen verschillende sancties staan. Zo kan de rechter uit de weigering een feitelijk vermoeden in zijn nadeel afleiden.[275]

De regel dat een partij zijn stelling ook moet bewijzen kan evenals naar Nederlands recht wordt verzacht door het zogenoemde vermoeden.[276] In beginsel kan dat op drie manieren. Ten eerste door bijzondere wetten. Ten tweede door wettelijke vermoedens en ten derde door een bewijs(last)overeenkomst. Voor de effectiviteit van watermerken zijn vooral de laatste twee verbijzonderingen van belang omdat er geen bijzondere wetten gelden voor de hier bedoelde situatie.

4.3.2 Aannemelijke verweren

De gedaagde doet er ook naar Belgisch recht verstandig aan verweer te voeren tegen de door eiser gestelde feiten en bewijsmiddelen om te voorkomen dat de rechter overtuigd raakt van het feit dat het bestand aan gedaagde toebehoort. Ten aanzien van het feit dat het bestand aan hem zou toebehoren kan hij in beginsel drie typen verweer voeren; toelaatbaarheidsverweren, betrouwbaarheidsverweren en verweren die zien op alternatieve verklaringen die mogelijk zijn ten aanzien van de stelling dat het op internet aangetroffen bestand naar hem verwijst.

Al deze verweren raken de effectiviteit van het watermerk op hun eigen manier. Wanneer het toelaatbaarheidsverweer slaagt zal de rechter het watermerk buiten beschouwing laten en is het niet langer in staat om het gestelde feit te bewijzen. Het watermerk is ook niet effectief wanneer het wel is toegelaten tot het bewijs maar de gedaagde erin slaagt de betrouwbaarheid van het watermerk als bewijsmiddel te weerleggen. Beide verweren raken direct de effectiviteit van het watermerk als juridisch bewijsmiddel en worden ook naar Belgisch recht apart behandeld in respectievelijk hoofdstuk 5 en 6.

Verweer voeren op grond van een alternatieve verklaring is ook naar Belgisch recht mogelijk maar niet eenvoudig. De gedaagde zal namelijk in het licht van de reeds genoemde en wellicht vaststaande en bekende feiten met een alternatief scenario moeten komen. Hij zal dit scenario ook voldoende moeten onderbouwen.[277] Het suggereren van de mogelijkheid van een virus of hack zal in de regel onvoldoende zijn als de gedaagde niet tevens concrete feiten aanvoert die daarop wijzen. Dit geldt overigens ook ten aanzien van de betrouwbaarheid van het watermerk. Ook daar zal de gedaagde zijn stellingen ten aanzien van de onbetrouwbaarheid van het watermerk moet onderbouwen. Hij zal duidelijk moeten maken dat het

[274] Zie in België art. 877 Ger.W. In Nederland geldt hetzelfde via art. 22 Rv.
[275] Zie uitgebreid Allemeersch 2007 (diss.), p. 442.
[276] Cattoir 2013, p. 84. Vermoedens vormen een bewijsmiddel op grond waarvan de rechter tot zijn eindoordeel mag komen.
[277] Allemeersch 2007 (diss.), p. 397.

watermerk niet alleen in theorie vervalst is maar ook dat het in het licht van andere bewijzen of vastgestelde feiten een realistisch scenario is.

Het onderbouwen van een alternatief scenario zal in de regel niet eenvoudig zijn. Dat kan gelegen zijn in het feit dat er geen bewijs is, maar ook omdat de kosten om het feit te bewijzen hoger liggen dan bijvoorbeeld de vordering. Hiermee is dan vanzelfsprekend niet gezegd dat het feit zich niet heeft voorgedaan. Zo is het bijvoorbeeld niet eenvoudig om te bewijzen dat je gehackt bent. Niet alleen kan de hack zelf gewoon zeer goed zijn uitgevoerd waardoor het lastig is om dit aan te tonen, maar ook heb je in veel gevallen een deskundige nodig om concrete feiten of bewijs aan te kunnen voeren.[278]

Evenals naar Nederlands recht is er ook naar Belgisch recht geen jurisprudentie voorhanden die duidelijk maakt wat de lijn zal zijn die rechters volgen. Het is ook naar Belgisch recht niet ondenkbaar dat wanneer de gedaagde een alternatief scenario als verweer aanvoert de rechter of de wederpartij in haar stellingen zal kiezen voor een zorgplicht om de computer toereikend te beveiligen of anders de gevolgen ervan te dragen. Dit zou kunnen onder verwijzing naar Frans recht waar in de inmiddels teruggetrokken Hadopi wetgeving ook een zorgplicht is aangenomen. Zij het dat in deze bestuurs-strafrechtelijke wetgeving de downloader aan zijn zorgplicht heeft voldaan indien hij zich houdt aan de aanwijzingen van zijn provider en de aanvullende lijst vanuit het ministerie die tot aan de dag van intrekking niet was opgesteld.[279] Ook naar Nederlands recht zijn er aanwijzingen te vinden voor het aannemen van een zorgplicht (zie par. 4.2.2.3), maar minder duidelijk dan bovenstaande gevallen. Met het aannemen van de zorgplicht zal de gedaagde duidelijk moeten maken dat hij aan de zorgplicht heeft voldaan. In hoeverre daarvan sprake is is afhankelijk van de omstandigheden van het geval. In die gevallen waarin men de rechter heeft kunnen overtuigen van een realistisch alternatief scenario en erin is geslaagd om duidelijk te maken dat hij aan zijn zorgplicht heeft voldaan kan het watermerk niet als een effectief bewijsmiddel worden gekwalificeerd. Een alternatief scenario presenteren als verweer is niet onmogelijk maar zal in de praktijk lastig zijn. Niet in de laatste plaats omdat de gedaagde zelf over de deskundigheid moet beschikken om voldoende verweer te kunnen voeren. Wanneer hij niet zelf over deze deskundigheid beschikt dan zal hij een deskundige moeten raadplegen (zie par. 4.3.3.2).[280]

4.3.3 Beslissen over feiten: het bewijsoordeel

Evenals naar Nederlands recht is het ook in België uiteindelijk aan de rechter overgelaten om in het licht van de stellingen van partijen het bewijs te waarderen en een oordeel te vormen over het gestelde feit. Wanneer de gedaagde betwist dat het bestand daadwerkelijk naar hem

[278] Dit staat nog los van de vraag of je nog beschikt over de bron. Zo zal het lastig zijn een verweer te baseren op een hack op je oude computer (smartphone) wanneer je deze niet meer in bezit hebt.
[279] Deze zorgplicht kan ook aangenomen worden onder verwijzing naar jurisprudentie van het BGH 12 mei 2010, I ZR 121/08 (Sommer unseres Lebens) over aansprakelijkheid inzake slecht beveiligde WLAN.
[280] Overigens is het niet ondenkbaar in zaken zoals deze dat veel internetfora bereid zullen zijn om met de gedaagde mee te denken.

wijst wordt de rechterlijke overtuiging ten aanzien van het watermerk van belang. Alleen dat bewijs hangt immers geheel van het watermerk af.

Om tot een beslissing te kunnen komen zal de rechter moeten nagaan of hij vrij is in de waardering van het watermerk of dat er beperkingen zijn gesteld aan de waardering daarvan (par. 4.4.3.1). De rechter kan zich bij het waarderen van het watermerk te allen tijde laten voorlichten door een deskundige (par. 4.4.3.2).

4.3.3.1 Beslissen over watermerken

De wetgever heeft de rechter evenals in Nederland wel enigszins beperkt in de waardering van het bewijs.[281] Ten eerste door de waardering te beperken tot wettige bewijsmiddelen.[282] Ten tweede door aan sommige bewijsmiddelen een bepaalde bewijskracht toe te kennen. Ten derde doordat de rechter zijn beslissing in zijn uitspraak moet motiveren.[283] Dit dient er mede toe om te controleren of de rechter zijn beslissing niet gebaseerd heeft op persoonlijke kennis van de feiten.[284] Ook het Hof van Cassatie laat het waarderen van de feiten over aan de feitenrechter, waardoor deze behoudens motiveringsklachten, niet vatbaar zijn voor cassatie.[285] De rechter is verder vrij in de wijze waarop hij tot zijn beslissing komt. Hij mag voor zijn beslissing ten aanzien van een feit steun zoeken in zijn persoonlijk geweten en gezond verstand inclusief de ervaringsregels, algemeen bekende feiten en zijn oordeel over de houding van partijen.[286] De rechter is met andere woorden vrij om zijn overtuiging te volgen bij het vaststellen van feiten.[287]

Door het gesloten systeem van bewijsmiddelen is de bewijskracht in beginsel ook bij wet bepaald. De bewijskracht bestaat uit de wettelijk opgelegde bewijswaarde van de middelen die de rechter tot het bewijs heeft toegelaten.[288] Enkel aan de betekenis, de eed, akte en wettelijke vermoedens is wettelijke bewijskracht toegekend. De wettelijke bewijskracht geldt zolang de wederpartij niet slaagt in het tegenbewijs. Getuigenverklaringen, feitelijke vermoedens en afschriften kennen een vrije bewijswaarde. Aan het watermerk is derhalve een vrije bewijskracht toegekend.

Evenals in Nederland is de rechter ook in België niet vrij in zijn oordeel wanneer partijen een bewijsovereenkomst sluiten waarin zij afspraken hebben gemaakt over de bewijspositie en

[281] Zie ook Allemeersch 2007 (diss.), p. 463.
[282] Cass. 11 december 1969. A.C. 1970, 357; Cass. 14 januari 2000, A.C. 2000, 109.
[283] Deze regel geldt als bijzondere toepassing van de motiveringsplicht (art. 149 Gw) dat haar oorsprong uiteindelijk vindt in het algemeen rechtsbeginsel van het recht op verdediging. Allemeersch 2007 (diss.), p. 466.
[284] Cass. 27 februari 1989. A.C. 1988-89, 735.
[285] Zie o.m. Laenens e.a. 2012; Zie o.m. Cass. 3 mei 2010, AR. S.009.0024.N, ov. 5.
[286] Allemeersch 2007 (diss.), p. 464; Cass. 17 december 1998, A.C. 1998-99, 1141, RW 1998-99, 1144, m.nt. F. Swennen.
[287] Allemeersch 2007 (diss.) p. 463.
[288] Cattoir 2013, p. 155; Samyn 2012, p. 51; Wagner 2009, p. 158.

bewijsmiddelen.[289] Maar zoals eerder opgemerkt zal dat bij watermerken geen bijzondere positie opleveren bij de inzet van watermerken. Ook in België wordt de mogelijkheid om ten nadele van consumenten af te wijken immers beperkt door dwingend recht. Zo is het ook in België onrechtmatig om in een consumentenovereenkomst bepalingen op te nemen die de bewijsmiddelen waarop de consument een beroep kan doen op ongeoorloofde wijze beperken of hem een bewijslast opleggen die normaliter op een andere partij bij de overeenkomst rust.[290] Het watermerk kan als bewijsmiddel ook in de overeenkomst worden opgenomen als een toegelaten bewijsmiddel. In de praktijk wordt vaker op deze manier een oplossing gevonden, om meer rechtszekerheid te verkrijgen dat een nieuw technisch bewijsmiddel ook zal worden toegelaten.[291]

Het is uiteindelijk aan de rechter om te beslissen over het geschil dat aan hem is voorgelegd. Wanneer beide partijen geloofwaardig stellingen en bewijzen hebben aangevoerd moet hij beslissen welke stellingen hij het meest geloofwaardig acht. De vraag is dan welke maatstaf hij moet hanteren bij de beoordeling van het bewijs.

Wagner merkt op dat de innerlijke overtuiging van de rechter wordt gevormd aan de hand van het geheel van de elementen van het dossier, aangevuld met feiten van algemene bekendheid en ervaringsregels.[292] Cijfermatige elementen (statistiek, kansberekening) zoals bij verslagen van gerechtsdeskundigen komen volgens hem weinig aan de orde in burgerlijke procedures.

De Belgische wetgever heeft evenals de Nederlandse geen maatstaf opgenomen voor het waarderen van bewijs. De rechter mag, behoudens wettelijke uitzonderingen, zelf bepalen welke waarde hij aan een bewijsmiddel toekent en wanneer het bewijs is geleverd. De rechter heeft de vrijheid om op onaantastbare wijze het bestaan van feiten vast te stellen en ook de gevolgtrekkingen die hij daaruit als vermoeden afleidt zijn aan zijn oordeel en beleid overgelaten. Hij mag echter niet aan de door hem vastgestelde feiten gevolgen verbinden die daarmee in geen enkel verband staan of die, op grond van die feiten, onmogelijk kunnen worden verantwoord.[293]

Algemeen wordt aangenomen dat wie in het recht bewijs wil leveren geen wetenschappelijke maar gerechtelijke zekerheid moet beogen.[294] Dat wil zeggen dat er een hoge graad van waarschijnlijkheid moet zijn, in overeenstemming met de normale gang van zaken, zodat de rechter niet ernstig meer aan het tegendeel moet denken, ook al is dit theoretisch nog

[289] Cattoir 2013, p. 577; Laenens e.a. 2012, p. 534; Allemeersch 2007 (diss.), p. 467.
[290] Zie o.m. art. 74 onder 21 WMPC (Wet betreffende marktpraktijken en consumentenbescherming); Laenens e.a. 2012, p. 534; Cattoir 2013, p. 585.
[291] Cattoir 2013, p. 580.
[292] Wagner 2009, p. 154.
[293] Cass. 3 mei 2010, AR. S.009.0024.N, ov. 5.
[294] Zie o.m. Mougenot 1997, p. 62; Allemeersch 2007 (diss.), p. 325; Wagner 2009, p. 154.

mogelijk.[295] De overtuiging van de rechter hoeft dan ook niet te steunen op wetenschappelijk-empirische zekerheid, maar slechts op redelijke zekerheid.[296]

In de rechtspraak wordt volgens vaste cassatierechtspraak een zeker bewijs vereist voor het vaststellen van feiten.[297] In zowel de feitenrechtspraak als de literatuur wordt algemeen aangenomen dat behoudens de wettelijke beperkingen, de rechter voor het vaststellen van de feiten doorgaans genoegen kan nemen met het bewijs van afdoende waarschijnlijkheid.[298] Om onredelijke gevolgen van een te strikte toepassing van de verdeling van de subjectieve bewijslast te voorkomen neemt het Hof van Cassatie genoegen met het bewijs van afdoende waarschijnlijkheid bij de vaststelling van negatieve feiten of positieve feiten waarvan een zeker bewijs onmogelijk kan worden geleverd.[299] Bijvoorbeeld via feitelijke vermoedens uit zeker bewijs van een ander positief feit. De voorlopige ondergrens ligt bij het 'aannemelijk maken', nu het Hof van Cassatie dat ten aanzien van het bewijs van een negatief feit onvoldoende achtte.[300]

Allemeersch merkt op dat de bewijsstandaard hiermee nagenoeg volledig subjectief wordt ingevuld. Hij geeft aan dat in andere landen weliswaar theoretisch pogingen zijn ondernomen om tot een objectievere invulling te komen, maar dat in de praktijk in die landen de rechterlijke beoordelingsvrijheid niet ingrijpend lijkt ingeperkt.[301] Tot slot kan er in het kader van de procedure nog op worden gewezen dat, zoals Stijns stelt, procespartijen meer belang hechten aan de conflictoplossende waarde van een gerechtelijke uitspraak dan aan het waarheidsgehalte daarvan.[302] De taak van de rechter is dan het toepassen van het recht op een feitelijke context die hij zo goed als redelijkerwijs mogelijk is op zijn waarachtigheid heeft getoetst.[303] Ook in die gevallen waarin partijen zelf het probleem niet volledig doorgrond hebben. Hiermee lijkt de zekerheid die in België van de rechter wordt verwacht bij het vaststellen van een feit niet te verschillen met die in Nederland.[304]

4.3.3.2 De deskundigen als betrouwbare informant

In 2009 is door middel van een reparatiewet het deskundigenonderzoek in het civiele recht nader bepaald en aangepast op de dagelijkse praktijk.[305] Ook naar Belgisch recht kan de

[295] Van Gerven 1969, p. 361; Ronse e.a 1988 schade, p. 76. gaven aan dat de schade zeker zal zijn wanneer ze in een zo hoge mate waarschijnlijk is, dat de rechter niet ernstig meer aan het tegendeel moet denken, ook al is dit theoretisch mogelijk; Zie ook Laenens e.a. 2012, p. 531.
[296] Zie o.m. Allemeersch 2007 (diss.), p. 466.
[297] Zie o.m. Cass. 2 maart 1956, A.C. 1956, 534; Cass. 23 oktober 2008, Pas. 2008, 2351. Zie ook Cattoir 2013, p. 111.
[298] Allemeersch 2007 (diss.), p. 466; Cattoir 2013, p. 111 en de daar aangehaalde literatuur.
[299] Idem.
[300] Cass. 26 november 2010, PAS, 2010, 3022.
[301] Zie o.m. Allemeersch 2007 (diss.), p. 465.
[302] Stijns 1990, p. 1005.
[303] Allemeersch 2007 (diss.), p. 583.
[304] Zie ook Allemeersch (2007 (diss.), p. 466) die stelt dat 'de overtuiging van de rechter niet moet steunen op wetenschappelijk-empirische zekerheid, maar slechts op redelijke zekerheid'.
[305] Wet van 30 december 2009 houdende diverse bepalingen betreffende justitie (B.S. 15 januari 2010).

rechter een deskundige gelasten vaststellingen te doen of een technisch advies te geven (art. 962 Ger. W.).[306] De rechter kan de deskundige ambtshalve of op verzoek van partijen horen. Dat geldt zowel voor de door de rechter aangestelde deskundige als de technische raadgevers van partijen (art. 985 Ger. W.). De rechter mag slechts afwijken van de keuze van partijen met een met redenen omklede beslissing. De deskundigen geven alleen advies over de in het vonnis bepaalde opdracht, tenzij partijen daarover overeenstemming bereiken (art. 962 Ger. W.). Evenals naar Nederlands recht is alleen de rechter bevoegd uitspraak te doen over de grond van de zaak en mag hij de zaak niet aan anderen delegeren (art. 11 lid 1 Ger. W.).[307]

Hoewel de rechter ook zelf een deskundige kan benoemen heerst het idee dat partijen de leiding hebben en het dus ook samen eens moeten worden over de inzet van de deskundige. De rechter kan een installatievergadering bijeen roepen waarin de rechter, partijen en de deskundige over het onderzoek inclusief de vraagstelling en andere kaders kunnen overleggen. Omdat dit in de praktijk niet altijd plaatsvond heeft de wetgever bij de laatste wetswijziging deze vergadering als facultatief opgenomen. Wanneer de rechter zelf en los van partijen besluit om een gerechtelijk deskundige in te zetten dan zal deze na acceptatie van zijn opdracht in beginsel samen met eventueel de experts van partijen om tafel gaat zitten om het in dit geval gedane onderzoek te bespreken. Het is uiteindelijk de gerechtelijk deskundige die na het debat hierover de eindbeslissing neemt en daarover rapporteert aan de rechter.

De waarborgen rondom de gerechtelijk deskundige kunnen worden gevonden in de beëdiging en de mogelijkheid hem te wraken.[308] Nadere regelingen zijn te vinden in art. 962-991 Ger. W. waar onder meer de aanstelling, wraking, verloop van het onderzoek en het organiseren van tegenspraak is geregeld. Deskundigen vervullen hun plicht onder toezicht van de rechter (art. 973 Ger. W.). Partijen zijn in beginsel verplicht mee te werken aan deskundigenonderzoeken, onder meer door relevante stukken te overleggen. Bij weigering kan de rechter daar zijn conclusies uit trekken (art. 972bis Ger. W.).

De beoordeling van de deskundigheid is uiteindelijk aan de rechter overgelaten.[309] De rechter bepaalt zelf de bewijswaarde van het deskundigenverslag en is daarmee vrij steun te vinden in het verslag, het verslag terzijde te stellen of bepaalde onderdelen daaruit te gebruiken.[310] Evenals naar Nederlands recht heeft de inzet van een deskundige(nverslag) in België geen bijzondere status en geldt ook hier dat de rechter vrij is in de waardering ervan. De wet staat

[306] Hoofdstuk VIII (Bewijs), afdeling 6 (art. 962-991bis) Ger. W. De regelingen rondom het deskundigenonderzoek zijn zowel voor civiel- als voor strafzaken grondig gewijzigd bij wet van 2007 en 2009. Wet van 15 mei 2007 tot wijziging van het Gerechtelijk Wetboek betreffende het deskundigenonderzoek en tot herstel van artikel 509quater van het Strafwetboek, B.S. 22 augustus 2007; Wet van 30 december 2009 houdende diverse bepalingen betreffende Justitie (II), B.S. 15 januari 2010. Zie voor een kritische beschouwing over deze wet inclusief deze laatste reparatiewet: Scheers & Thiriar 2010. En voor de lessen naar Nederlands recht Krans & Santing-Wubs 2012. De rechter is niet verplicht tot in het aanstellen van een deskundige Cass. 15 juni 2012, AR C.11.0721.F

[307] Laenens e.a. 2012, p. 590.

[308] Art. 985 lid 2 Ger. W.; art. 966 GerW.

[309] In het verleden zijn er wel meerdere voorstellen geweest, zowel in het civiel als in het strafrecht.

[310] Zie Cass. 22 januari 2008, NC 2008, 140; Cass. 7 mei 2009, A.C. 2009, 1196, 1108; Laenes e.a. 2012, p. 593.

er dan ook niet aan in de weg dat de rechter de juistheid van de technische vaststellingen van de deskundige niet meer zou kunnen beoordelen.[311] De rechter is ook niet verplicht het advies van de deskundigen te volgen wanneer dit in strijd is met zijn overtuiging (art. 962 Ger. W.). De rechterlijke overtuiging geldt daar als beslissende toetssteen, stelt Allemeersch.[312] Niettemin zal de rechter zich volgens Boularbah in werkelijkheid beperken tot een marginale toetsing van het werk van de deskundige en een toepassing van het recht op de resultaten van zijn werk.[313] De Belgische rechter lijkt hiermee in zijn beoordeling meer ruimte te krijgen dan zijn Nederlandse collega om van het deskundigenverslag af te wijken. In de praktijk zal dit echter weinig uitmaken omdat ook de Belgische rechter zich geconfronteerd ziet met een deskundige die hetzij door partijen hetzij door hemzelf is gebruikt om hem voor te lichten over zaken waarvoor een specifieke deskundigheid is vereist. De rechter zal het oordeel van de deskundigen in de praktijk dan niet snel terzijde schuiven. Dat zal voor het verslag van deskundigen inzake watermerken niet anders zijn.

Evenals naar Nederlands recht ligt de inzet van een door de rechter aangestelde deskundige in het kader van een onderzoeksmaatregel bij watermerken niet voor de hand vanwege mogelijke vertragingen en de kosten.[314] Ten aanzien van het deskundigenonderzoek geldt het subsidiariteitsbeginsel.[315] Dat betekent dat de rechter zich bij een keuze van een onderzoeksmaatregel moet beperken tot wat volstaat om het geschil op te lossen, waarbij de meest eenvoudige, snelle en goedkope maatregel de voorkeur geniet.[316] De rechter dient alvorens tot een deskundigenonderzoek over te gaan zich eerst af te vragen of hij zich op een andere wijze kan laten voorlichten. Bijvoorbeeld op grond van de stukken van een of beide partijen. In de praktijk beoordeelt de rechter allereerst of de inbreng van een gerechtelijk deskundige opportuun is en of deze in overeenstemming is met de waarde van het geschil.[317] Dit tegen de achtergrond dat een deskundigenonderzoek aanzienlijke kosten met zich meebrengt, de procedure vertraagt en bijdraagt aan de gerechtelijke achterstand.[318] Door de waarde van het geschil in verhouding met kosten die gepaard gaan met de inzet van (gerechtelijk) deskundigen te bepalen kan de rechthebbende met name een strategisch voordeel behalen. Door de waarde van het geschil relatief laag te houden kan de rechthebbende in de praktijk de inzet van de andere deskundige beperken. De rechter zal immers bij een geringe waarde geen gerechtelijk deskundige benoemen en ook de gedaagde zal na moeten denken of de kosten van een partijdeskundigen opwegen tegen het (onzekere) resultaat. Bij geringe vorderingen is het derhalve niet ondenkbaar dat andere deskundigen in

[311] Cass. 21 januari 2011, Pas. 2011, 234; Laenes e.a. 2012, p. 593.
[312] Allemeersch 2007 (diss.), p. 465
[313] Boularbah 2008, p. 7.
[314] Onderzoek (Justitiebarometer 2014 uitgevoerd door Phonecom) naar de houding van de Belgische bevolking (niet perse deelnemers aan het rechtsverkeer) ten aanzien van justitie laat zien dat in burgerlijke zaken 90% van de ondervraagden het belangrijk vindt om deskundigen aan te stellen ook al wordt de duur hierdoor langer en 81% van de ondervraagden vindt het belangrijk om deskundigen in te schakelen ook al worden de kosten hierdoor hoger.
[315] Scheers & Thiriar 2008, p. 123.
[316] Art. 875bis Ger.W., ingevoegd bij de wet van 15 mei 2007 betreffende het deskundigenonderzoek.
[317] Zie ook artikel 991 lid 2 Ger. W.
[318] Castermans 2007, p. 12-13.

de praktijk buiten spel worden gezet. Hierbij moet worden opgemerkt dat in België de rechter de erelonen van de deskundigen bepaalt (art. 987-991bis Ger. W.). Deze liggen in het algemeen lager dan in Nederland waar de markt meer regeert.

Ook in België kan dan een schikking voor een partij een veel aantrekkelijker alternatief zijn dan het voeren van een procedure waarvan de uitkomst ook met de inbreng van deskundigen onzeker is. Dat is ook het geval waarin de gedaagde objectief gezien het bestand niet op internet heeft gezet. In dit geval is er naar mijn mening in beginsel niet direct sprake van bewijsnood. Het is in dit geval de gedaagde zelf die ervoor kiest om geen kosten te maken om bewijs te leveren. Het is anderzijds ook niet ondenkbaar dat de rechter de gedaagde tegemoet komt als ware het bewijsnood in het geval de verhoudingen van partijen daartoe aanleiding geven. Bijvoorbeeld in het geval de rechthebbende een grote repeatplayer is en de gedaagde een gewone consument. Die verhouding ligt anders wanneer het een individuele beroepsfotograaf is tegenover een consument. In dat geval zou het onredelijk zijn om de consument tegemoet te komen. Tegenover de kosten van de inzet van de deskundige staan immers ook de kosten die de fotograaf heeft moeten maken om het watermerk in te zetten. Het is overigens lastig om deze zaken scherp te stellen, omdat in een procedure veel meer elementen een rol spelen bij een redelijke verdeling, zoals de houding van procespartijen en feiten die mogelijk al wel zijn vastgesteld. In die verhouding kan het spiegelbeeld optreden dat het onredelijk is om de consument te beschermen tegen een repeatplayer. Hoewel dat theoretisch onbevredigend is speelt de vrijheid van de rechter om zaken individueel te beoordelen terecht een grote rol. Alleen ter zitting kan bepaald worden wat redelijk is in een gegeven geval. In de praktijk zal dit zeker niet altijd tot het meest bevredigende resultaat leiden, mede vanuit het oogpunt van rechtszekerheid. Aan de andere kant kan er ook op worden gewezen dat veel mensen in zowel Nederland als België niet ontevreden zijn over de uitkomsten van rechtszaken en vertrouwen hebben in rechters.[319]

4.3.4 Tussenconclusie

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te beoordelen is het watermerk in de context van het Belgische civiele bewijsrecht geplaatst. De effectiviteit van bewijsmiddelen wordt daar beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en welke stellingen over dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd.

Ook naar Belgisch recht geldt als uitgangpunt dat het aan partijen is overgelaten om door middel van onderbouwde stellingen de omvang en inhoud van het geschil te bepalen. Het is uiteindelijk aan de rechter overgelaten om het feit al dan niet vast te stellen. Om tot een

[319] Vertrouwen in de rechtspraak blijkt lastig te meten, zoals ook Corstens concludeert voor met name de Nederlandse situatie.
http://www.rechtspraak.nl/Organisatie/HogeRaad/OverDeHogeRaad/publicaties/Pages/Vertrouweninderechtspraak.aspx. Zie voor België, de laatste Justitiebarometer (2014).

beslissing te kunnen komen heeft de wetgever een stelsel in het leven geroepen waarin duidelijk wordt wie het bewijsrisico draagt wanneer het feit niet komt vast te staan.

In dit stelsel draagt in de gegeven casus de rechthebbende de bewijslast ten aanzien van het door hem te stellen feit dat het bestand aan de licentienemer toebehoort. Hij zal onder meer op grond van de medewerkingsplicht het watermerk in de vorm van een rapportage direct bij de stukken aanvoeren ter onderbouwing van zijn stelling. Om te voorkomen dat de rechter dit feit direct vaststelt zal de gedaagde (licentienemer) dit feit voldoende moeten betwisten. De rechthebbende zal daartoe in zijn rapportage voldoende aanknopingspunten moeten bieden aan de licentienemer. Evenals naar Nederlands recht heeft de gedaagde bij gebrek aan medewerking eventueel met de hulp van de rechter voldoende middelen om bewijs aan te voeren dan wel een contra-expertise uit te (laten) voeren.

De gedaagde kan ten aanzien van het watermerk in het licht van het gestelde feit in beginsel drie verweren voeren. Ten aanzien van het watermerk kan hij verweren voeren die de toelaatbaarheid en/of betrouwbaarheid van het watermerk betwisten. Beide verweren raken direct de effectiviteit van het watermerk dat erin bestaat dat het gestelde feit kan worden vastgesteld. Ten aanzien van het gestelde feit kan de gedaagde de positie innemen dat er alternatieve verklaringen bestaan voor het openbaar worden van het bestand, bijvoorbeeld doordat iemand anders dat heeft gedaan. Dit laatste verweer raakt de effectiviteit van het watermerk niet. De rechter kan het feit immers vaststellen. De gedaagde betwist hier het verband tussen het op internet aangetroffen bestand en zijn schuld. Het is immers aan de rechthebbende om te stellen en zo nodig te bewijzen dat zijn werk openbaar is gemaakt door de gedaagde. Zonder die vaststelling is er geen sprake van inbreuk op het auteursrecht. Voor een succesvol verweer dient de gedaagde zijn stelling dat er sprake is van een alternatieve verklaring wel te onderbouwen. Zo zal hij bijvoorbeeld ten aanzien van een hack moeten onderbouwen waarom hiervan sprake zou zijn. Bijvoorbeeld met behulp van een onderzoek waarin blijkt dat er rond het opgegeven tijdstip sporen van een hack zijn gevonden.

Wanneer de rechter van oordeel is dat partijen voldoende hebben gesteld en betwist, kan de rechter ook nog een deskundigenbericht vragen wanneer hij graag meer informatie zou willen over een punt waarover partijen nog van mening verschillen. Partijen kunnen daarop reageren. Tot slot geeft de rechter een definitief bewijsoordeel dat in dialoog met partijen tot stand is gekomen. De bewijsbeslissing is daarmee tot stand gekomen binnen de ruimte die de stellingen van partijen hebben gelaten.

De rechter is bij gebrek aan wettelijke bepalingen ten aanzien van de waardering van watermerken vrij in de waardering ervan. Ook in de jurisprudentie zal de rechter geen steun vinden voor de waardering van watermerken. Het komt ervoor de rechter dan op aan om zelf tot een oordeel te komen, eventueel met de hulp van een door hemzelf benoemde deskundige dan wel op basis van de door partijen ingebrachte verslagen, experts of andere materialen. In

de praktijk zal de rechter zijn beslissing veelal, mede in het licht van het financiële belang van de zaak, beoordelen in het licht van hetgeen partijen hebben ingebracht.

4.4 Beslissen over feiten naar Nederlands strafrecht

Als uitgangspunt geldt dat het aan het Openbaar Ministerie (hierna: OM) is om de verdachte een strafbaar feit ten laste te leggen en om te bewijzen dat hij het tenlastegelegde feit heeft begaan.[320] De rechter kan slechts aannemen dat de verdachte het tenlastegelegde feit heeft begaan wanneer hij daarvan uit het onderzoek op de terechtzitting "door den inhoud van wettige bewijsmiddelen de overtuiging heeft bekomen" (art. 338 Sv). In tegenstelling tot het Nederlands civiel recht is de strafrechter niet lijdelijk maar speelt hij een actieve rol bij de juridische waarheidsvinding. Hij leidt het onderzoek ter terechtzitting.

Het vaststellen van feiten is aan de rechter overgelaten. Hij kan de feiten onderzoeken door bestudering van het dossier en het onderzoek ter terechtzitting.[321] De bewezenverklaring moet uiteindelijk berusten op wettige bewijsmiddelen: eigen waarneming van de rechter, verklaring van de verdachte, getuige of deskundige en het schriftelijk stuk. Ten aanzien van feiten stelt de wet weinig nadere eisen. Evenals in het Nederlandse civiel bewijsrecht is het uiteindelijk aan de rechter overgelaten om te beslissen of het tenlastegelegde feit kan worden bewezen. De rechter kan het feit dat het bestand aan de licentienemer toebehoort in ieder geval bewezen verklaren wanneer verdachte (licentienemer) het feit heeft erkend in zijn verklaring.[322]

Evenals in het Nederlands civiel recht behoeven in het strafrecht feiten van algemene bekendheid geen bewijs (art. 339 lid 2 Sv). De wetgever heeft met de structurering van het onderzoek ter terechtzitting en met eisen van wettige bewijsmiddelen (art. 339 Sv), voorgeschreven bewijsminima (art. 352, lid 1 Sv) en de eis van de rechterlijke overtuiging (art. 338 Sv) beoogd de oordeelsvorming te kanaliseren en te objectiveren. Hiermee heeft hij een stelsel in het leven willen roepen dat de rechter noodzakelijke ruimte biedt om tot een kwalitatief hoogwaardig en betrouwbaar bewijsoordeel oordeel te komen.[323] De wetgever en daarmee het bewijsrecht gaat uit van een rechter die binnen de grenzen van het recht actief op zoek gaat naar de materiële waarheid.

[320] Het Nederlands strafrechtelijk bewijsrecht is voornamelijk geregeld in het Wetboek van Strafvordering (art. 338 Sv - 344a Sv) en vormt een nadere regeling van de eerste vraag van artikel 350 Sv. Zie hierover ook Nijboer 2011, p. 15. Het strafrecht moet tevens rechtsbescherming bieden tegen de overheid. Dat werkt door in het bewijsrecht. Zo worden in het strafrecht hogere eisen aan het bewijs gesteld dan in het dagelijks leven en geldt er een bewijsminimum van twee bewijsmiddelen.

[321] Uit onderzoek van Vrij Nederland (2013) onder rechter blijkt (V26_2) wel dat een meerderheid (59,6%) van de deelnemende rechters van mening is dat de (lange) duur van de zitting mede komt doordat de dossiers die door de politie worden aangeleverd incompleet en/of kwalitatief onvoldoende zijn.

[322] Zie art. 339 eerste lid Sv; Nijboer 2011, p. 180. Overigens hebben arresten rondom gerechtelijke dwalingen ons ook geleerd dat de rechter extra alert moet zijn wanneer de verdachte komt tot een verklaring en deze later intrekt.

[323] Zie o.m. Nijboer 2011, p. 72; Cleiren 2010, p. 263; Groenhuijsen 2004 p. 151.

Bij aanvang van de procedure is het aan het OM om te bewijzen dat de verdachte opzettelijk inbreuk heeft gepleegd op het auteursrecht van een ander (art. 31 Aw).[324] Het watermerk dient in een dergelijke procedure als bewijs dat het bestand aan de licentienemer toebehoort.

De effectiviteit van watermerken wordt naar Nederlands strafrecht beoordeeld in het licht van het door het OM te bewijzen feit dat het bestand aan de licentienemer toebehoort, en welke argumenten over dat feit en het watermerk door de verdachte zijn aangevoerd dan wel door de rechter zijn betrokken bij zijn beoordeling. In de praktijk volgt de rechter echter de ingebrachte rapportage wanneer de verdediging geen actieve bijdrage levert aan mogelijke verweren.[325]

Vanuit dit perspectief is het vooral zinvol om aandacht te besteden aan de vraag welke stellingen het OM moet en de verdachte redelijkerwijs kan aanvoeren over watermerken en op welke wijze de rechter deze stellingen moet beoordelen. Om die reden wordt eerst ingegaan op de vraag bij welke partij het bewijsrisico ligt wanneer de feiten onduidelijk blijven en hoe partijen hun stellingen kunnen onderbouwen (par. 4.4.1). Daarna wordt specifiek ingegaan op aannemelijke verweren die de verdachte kan aanvoeren om het watermerk ineffectief te maken (par. 4.2.2). Tot slot wordt gekeken naar vraag hoe de rechter tot zijn bewijsoordeel komt (par. 4.2.3). De paragraaf wordt afgesloten met een tussenconclusie (par. 4.2.4).

4.4.1 Bewijsrisicoverdeling

Het Nederlandse strafrecht kent in tegenstelling tot het Nederlandse civiel recht vooraf een duidelijke risicoverdeling. De stelplicht en daarmee het daarmee samenhangende bewijsrisico ligt altijd bij het OM. Anders dan in het civiel recht is louter de rechter verantwoordelijk voor de volledigheid en deugdelijkheid van het onder zijn leiding plaatshebbende onderzoek ter terechtzitting.[326] Ten aanzien van het bewijs gaat het louter om de oordeelsvorming van de rechter dat leidt tot een gemotiveerde bewezenverklaring of een vrijspraak.[327] De rechter is daarbij gebonden aan de wet maar niet aan standpunten van partijen.

Het uitgangspunt van het strafprocesrecht wordt gekenmerkt door het schuldbeginsel dat inhoudt dat de verdachte voor onschuldig wordt gehouden totdat zijn schuld rechtens is komen vast te staan (praesumptio innocentiae).[328] Van de verdachte kan dan ook niet worden gevraagd om zijn onschuld te bewijzen en in die zin rust er dan ook geen bewijslast op de verdachte, noch draagt hij het bewijsrisico.[329] Dit komt ook tot uiting in zijn procespositie. Hij is in zoverre vrij zijn positie te bepalen dat hij zelf zijn inbreng kan bepalen.[330] De verdachte

[324] Zie voor andere strafbare feiten par. 3.4.2.
[325] Zie par. 4.4.3.2.
[326] Zie o.m. Nijboer 2011, p. 159.
[327] Idem.
[328] Art 6 lid 2 EVRM; art. 14 lid 2 BUPO-verdrag.
[329] Zie o.m. Borgers & Kristen 1999.
[330] Zie o.m. Nijboer 2011, p. 163.

kan ervoor kiezen om verstek te laten gaan of zich te beroepen op zijn zwijgrecht. Ook in die gevallen is het de verantwoordelijkheid van de rechter om ook te kijken naar gegevens die ontlastend zijn voor de verdachte.[331] Anders dan in een civiel geschil leidt het niet voeren van een verweer niet per definitie tot de vaststelling van het gestelde feit. De rechter kan, anders dan in een civiel geschil, zich niet op het standpunt stellen dat hij passief moet blijven omdat de verdachte geen verweer heeft gevoerd. De bijdrage van de verdachte kan beperkt blijven tot het dulden of ondergaan van onderzoeken (art. 61a Sv). Hij heeft ook verschillende mogelijkheden om verklaringen af te leggen en invloed uit te oefenen op het verloop van het onderzoek (art. 263-331 Sv), zoals het stellen van vragen, inbrengen van stukken en dagvaarden en inbrengen van deskundigen. Hoewel de verdachte kan zwijgen zal het duidelijk zijn dat het voeren van verweer in veel gevallen zal bijdragen aan de wijze waarop de bewijsbeslissing uiteindelijk in het hoofd van de rechter tot stand komt.[332] De rechter kan bij het nemen van een bewijsbeslissing ook rekening houden met de houding van de verdachte tijdens het proces.[333] Dat risico zal voornamelijk intreden wanneer de verdachte weigert specifieke gegevens bekend te maken die in het domein van de verdachte liggen en waarvan het OM en de rechter anders geen kennis zouden hebben. Met dat zwijgen neemt hij het risico dat die gegevens geen rol spelen bij de oordeelsvorming.[334] In de regel zal een verdachte er goed aan doen verweer te (laten) voeren zodat de rechter expliciet gewezen wordt op de mogelijke verweren.

4.4.2 Aannemelijke verweren

Wanneer de verdachte besluit verweer te voeren dan zal zijn verweer zich richten tegen de bewezenverklaring van het tenlastegelegde feit. De rechter is als gevolg van artikel 359 lid 2 Sv verplicht aandacht te besteden aan deze bewijsverweren wanneer deze gelden als een uitdrukkelijk ingenomen standpunt.

Ten aanzien van watermerken als bewijsmiddel zijn evenals in het civiele recht in beginsel drie typen (hoofd)verweren te voeren; toelaatbaarheidsverweren, betrouwbaarheidsverweren en verweren die een alternatieve verklaring geven ten aanzien van het gestelde feit.[335] De eerste twee verweren raken direct de effectiviteit van het watermerk omdat de rechter zowel een ontoelaatbaar als een onbetrouwbaar watermerk uiteindelijk niet als juridisch bewijs zal

[331] Zie o.m. Nijboer 2011, p. 164.
[332] Zie in par. 4.4.3.2 voor het belang van zijn inbreng voor de beoordelen van rapporten ten aanzien van het watermerk.
[333] Nijboer 2011, p. 164; EHRM 8 februari 1996, NJ 1996, 725 (Murray). De enkele omstandigheid dat de verdachte in het voorbereidend onderzoek geen verklaring heeft willen afleggen mag echter niet in zijn nadeel werken ten aanzien van het bewijs van het tenlastegelegde feit (HR12 maart 1996, NJ 1996, 539).
[334] Nijboer 2011, p. 165.
[335] Vooral toelaatbaarheidsverweren worden volgens Nijboer (2011, p. 171) dikwijls aangevoerd. Onderzoek van Van Buskirk & Liu 2006 laat in de Verenigde Staten zien dat partijen veelal de voorkeur geven aan het voeren van verweer ten aanzien van de juridische toelaatbaarheid in plaats van verweer ten aanzien van de betrouwbaarheid. Kessler (2010 (diss.), p. 9) merkt op dat er tot 2010 geen ander onderzoek is dat thans op andere conclusies zou wijzen. In Nederland is mij geen (ander) onderzoek bekend.

accepteren.[336] Het laatstgenoemde verweer raakt het watermerk als bewijsmiddel in beginsel niet. Wanneer de rechter het feit kan vaststellen met behulp van het watermerk is het watermerk immers effectief te noemen. Toch zal de waarde van het watermerk als bewijs- en handhavingsmiddel sterk afnemen wanneer het in de praktijk eenvoudig blijkt om met een alternatieve verklaring te komen ten aanzien van het door het watermerk bewezen feit. In deze paragraaf zal vooral aandacht worden besteed aan dit laatste type verweer. De eerste twee typen verweren worden vanwege hun directe belang voor de effectiviteit van het watermerk in de volgende twee hoofdstukken nader besproken.

Een verweer dat ziet op een alternatieve verklaring van het gestelde feit is ook in het strafrecht in beginsel een aantrekkelijk verweer. De verdachte voert dan immers geen verweer tegen de toelaatbaarheid en betrouwbaarheid van het watermerk maar geeft een andere lezing van het gebeurde. Het verweer moet dan wel zien op een situatie die niet onwaarschijnlijk is in het licht van hetgeen ter zitting reeds bekend is geworden en wel in strijd is met de tenlastelegging maar niet met de overige bewijsmaterialen. Dit wordt ook wel aangeduid als een meer- en vaart-situatie of een meer- en vaart-verweer.[337] De rechter mag verweren die voldoende concreet gemotiveerd zijn niet zonder nader motivering terzijde stellen.[338] Evenals in het civiele recht is het niet eenvoudig om deze verweren te voeren. De verdachte kan niet volstaan met de loutere stelling dat een alternatieve verklaring mogelijk is voor het feit dat het aangetroffen bestand zijn naam bevat. In de meeste gevallen zal het OM immers rekening hebben gehouden met mogelijke verweren en voldoende bewijs hebben aangedragen om dergelijke eenvoudige stellingen te voorkomen. De verdachte zal, om het bewijsoordeel van de rechter te beïnvloeden, er steeds goed aan doen om deze te motiveren. De kwaliteit van de motivering zal evenals in het civiele recht afhangen van de kwaliteit van de overige bewijsmiddelen en stellingen.

De bewijsvraag: heeft de verdachte het tenlastegelegde feit begaan?

Met de koppeling tussen het bestand en de verdachte (licentienemer) is het watermerk als bewijsmiddel weliswaar effectief te noemen ten aanzien van het gestelde feit maar rest evenals in het civiele recht de vraag of de beweerde schending van het auteursrecht door de verdachte is gepleegd. Hoewel het de effectiviteit van het watermerk indirect raakt zal kort op deze vraag worden ingegaan. Het OM zal immers moeten bewijzen dat de verdachte opzettelijk inbreuk maakt op het auteursrecht van een ander (art. 31 Aw).[339]

[336] Verweren ten aanzien van de betrouwbaarheid van watermerken kunnen in beginsel al slagen door het zaaien van twijfel ten aanzien hiervan. Om die twijfel te kunnen zaaien zal in veel gevallen de hulp van een deskundige nodig zijn. Wanneer het verweer niet onaannemelijk is maar er in het licht van andere bewijsmiddelen wel twijfels zijn kan het voor de rechter aanleiding zijn om nader onderzoek te (laten) verrichten.
[337] Zie o.m. Nijboer 2011, p. 171.
[338] Art. 359 lid 2 Sv. Zie Nijboer 2011, p. 170 en de daar aangehaalde arresten.
[339] Zie voor de andere strafrechtelijke delicten par. 3.4.2.1. De vraag of met een koppeling tussen de verdachte en het bestand ook de noodzakelijke opzet is bewezen wordt verder buiten beschouwing gelaten.

De vraag naar de wijze waarop het aangetroffen spoor (het bestand) daar is gekomen speelt, naast in de forensische IT, ook in andere domeinen van forensisch onderzoek een belangrijke rol.[340] De vraag in welke mate dit een rol speelt ten aanzien van auteursrechtinbreuk door het uploaden van bestanden is lastig te beantwoorden. Onderzoek naar jurisprudentie op rechtspraak.nl tussen 1990-2012 levert uiteindelijk slechts vier inhoudelijk relevante uitspraken op.[341]

In deze zaken waarin het uploaden van bestanden een rol speelt, komt de rechter drie keer tot het bewijs dat de verdachte zelf direct bestanden heeft geüpload.[342] In een geval bekende de verdachte dat feit[343] en in twee andere zaken is er geen inhoudelijk verweer gevoerd tegen het uploaden van de bestanden.[344] De veroordelingen die volgen betreffen andere strafbare feiten, zoals medeplichtigheid[345] en medeplegen[346]. In al deze zaken gaat het om een verdachte die betrokken is geweest bij het faciliteren en verspreiden van auteursrechtelijk beschermde bestanden. Het uploaden door de verdachte speelt daarbij veelal een ondergeschikte rol omdat het OM de verdachte vooral (ook) andere strafbare feiten ten laste legt zoals deelname aan een criminele organisatie. Niettemin kan enig inzicht worden verkregen in de wijze waarop de rechter in deze zaken tot zijn beslissing kwam.

De rechtbank Rotterdam achtte in 2007 in de E-donkey zaak bewezen dat de verdachte (muziek)werken heeft geüpload door middel van het programma E-Mule (p2p-software).[347] De in het zogenoemde Brein-dossier opgenomen mededelingen (postings) door onder andere verdachte, maken het volgens de rechter weliswaar aannemelijk dat de werking van de website gericht is op het uploaden van bestanden, maar vormen geen zelfstandig bewijs dat door de verdachte zelf bestanden die auteursrechtelijk beschermde werken bevatten zijn

[340] Zie ten aanzien van IT o.m. Bhoedjang 2008, p. 378. Zie in andere domeinen (DNA, bloed, etc.) o.m. Broeders & Muller 2008. De vraag wie de digitale sporen heeft achtergelaten is echter bijzonder lastig te beantwoorden. Zie o.m. Bhoedjang 2008, p. 395.

[341] Hof Den Haag 18 januari 2013, ECLI:NL:GHDHA:2013:BZ6496, CR 2013/161 m.nt. J.J. Oerlemans, Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey), Rb. Amsterdam 11 september 2008, ECLI:NL:RBAMS:2008:BF0824 (Bandbreedte), Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5615 (FXP). Onderzoek op rechtspraak.nl naar strafzaken in de periode 1990-2012 met de trefwoorden [auteursrecht, upload] inclusief het meervoud hiervan. In totaal gaat het om zeven gepubliceerde uitspraken, soms met meerdere verdachten in één zaak waardoor meerdere uitspraken zijn gepubliceerd. De belangrijkste reden voor de beperkte jurisprudentie op dit terrein is m.i. dat schending van auteursrechten weinig aandacht krijgt van het OM. Voor andere strafbare feiten is het voor het bewijs vaak niet nodig om een verband te leggen tussen de upload van een enkel bestand en de uploader. In veel zaken staat het uploaden vast, veelal omdat het om meerdere bestanden gaat en de rechter uploaden aanneemt vanwege de (bittorent)techniek. Het betreft zaken van het landelijk parket en het gaat niet om individuele uploads van de consument.

[342] Jurisprudentie-onderzoek op rechtspraak.nl (30 december 2014) levert op de trefwoorden: auteursrecht en uploaden, 7 uitspraken op. In de andere twee zaken over hetzelfde feitencomplex (andere verdachte) kwam het Hof 's-Gravenhage, 22 december 2010, ECLI:NL:GHSGR:2010:BO8245, BO8246 (E-donkey) tot de conclusie dat het OM niet-ontvankelijk was op grond van de Aanwijzing intellectueel-eigendomsfraude.

[343] Hof Den Haag 18 januari 2013, ECLI:NL:GHDHA:2013:BZ6496, CR 2013/161 m.nt. J.J. Oerlemans.

[344] Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5610 (FXP); Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5615 (FXP).

[345] Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey).

[346] Rb. Amsterdam 11 september 2008, ECLI:NL:RBAMS:2008:BF0824 (Bandbreedte).

[347] Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey).

geüpload. Het bewijs voor het uploaden komt in deze zaak uit het digitaal onderzoek op de computer van de verdachte waarmee het gebruik van het programma E-mule voor de rechter was komen vast te staan. Vervolgens was uit het dossier en het verhandelde ter terechtzitting aannemelijk geworden dat bestanden die met behulp van het programma eMule gedownload worden ook direct weer ter beschikking worden gesteld voor het uploaden. De rechtbank achtte vervolgens wettig en overtuigend bewezen dat de verdachte opzettelijk inbreuk heeft gemaakt op het auteursrecht van anderen.

Deze zaak werd vooral bekend door het hoger beroep dat volgde, waarin het Hof 's-Gravenhage het OM op grond van de Aanwijzing (en inmiddels richtlijn voor strafvordering) intellectuele-eigendomsfraude niet-ontvankelijk verklaarde in de vervolging van de verdachte.[348] Aan de inhoudelijke behandeling van de zaak werd door het hof dan ook niet toegekomen.

De rechtbank Amsterdam achtte in een zaak in 2008 het uploaden van werken door verdachte zelf niet bewezen maar kwam tot een bewezenverklaring van deelneming aan een misdrijf. Inbreuk op het auteursrecht werd bewezen geacht doordat de verdachte in een studentenflat een computer voor uploaden beschikbaar had gesteld en het uploaden van films ook daadwerkelijk had plaatsgevonden door de mededader van verdachte.[349] Hoe het uploaden door de medeverdachte is komen vast te staan blijkt niet uit deze zaak.

In de FXP-board-zaak worden verdachten veroordeeld voor deelname aan een criminele organisatie met als oogmerk hacken en uitwisselen van auteursrechtelijk beschermde werken (art. 138a, 139d Sr en 31 Aw).[350] Het uploaden van bestanden door verdachte komt in deze zaak verder niet aan orde omdat het OM zich hier richt op het forum dat als oogmerk had het hacken van computersystemen om gebruik te maken van de schijfruimte en bandbreedte zodat er snel auteursrechtelijk beschermde werken konden worden geüpload en gedownload. In deze laatste zaak is hoger beroep ingesteld maar ook het hof acht onder meer op basis van eigen verklaringen en forensisch onderzoek bewezen dat verdachte heeft deelgenomen aan een organisatie die tot oogmerk had het plegen van inbreuk op het auteursrecht van anderen.[351]

[348] Hof 's-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010:BO8245; BO8246 (E-donkey).
[349] Rb. Amsterdam 11 september 2008, ECLI:NL:RBAMS:2008:BF0824 (Bandbreedte): De verdachte had 'in totaal vijf computers boven de plafondplaten geplaatst en aangesloten op de internetkabels om illegaal gebruik te kunnen maken van de internetverbinding van de studentenflat en bestanden te downloaden en verspreiden'.
[350] Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5610 (FXP); Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5615 (FXP).
[351] Hof Den Haag 18 januari 2013, ECLI:NL:GHDHA:2013:BZ6496, CR 2013/161 m.nt. J.J. Oerlemans.

Op basis van met name de E-donkey-zaak lijkt het uploaden van bestanden in bewijsrechtelijke zin een kwestie van goed forensisch onderzoek op de computer van de verdachte en ander bewijs zoals eigen verklaringen en het rechterlijk vermoeden.[352]

Zowel ten aanzien van het watermerk als van bewijs dat voortkomt uit forensisch onderzoek kan een verdachte altijd verweer voeren waarin hij het watermerk of de resultaten van het onderzoek niet betwist maar naar een andere oorzaak wijst. De verdachte zal dan vooral stellen dat hij geen idee heeft hoe het bestand op internet terecht is gekomen en dat iemand anders dat zonder zijn toestemming moet hebben gedaan, bijvoorbeeld terwijl hij zijn computer even had uitgeleend.[353] Deze argumenten zijn niet voorbehouden aan zaken waarbij het auteursrecht een rol speelt maar worden ook ingeroepen in zaken rondom kinderporno.[354]

Stevens & Koops onderzochten onder meer welke (alternatieve) verweren er werden gevoerd inzake kinderporno.[355] Op grond van dat en eigen onderzoek is verder gekeken naar de verweren die relevant kunnen zijn voor watermerken.[356]

Ten eerste kan de verdachte ontkennen dat hij het (muziek-, film-, foto-)bestand ooit heeft gehad. Dat verweer beoordeelt de rechter in relatie tot de andere feiten. Voor overwegingen ten aanzien van dergelijke verweren kan en zal eenvoudig aansluiting worden gezocht bij de overwegingen in zaken rondom kinderporno.[357] Dit verweer wordt hier verder dan ook niet besproken.

Ten tweede kan de verdachte zich beroepen op het zogenoemde hackers of Trojan verweer (hackers-defence).[358] Met dit verweer wijst de verdachte op een hacker die de computer van verdachte ongewild heeft gebruikt om bestanden te verspreiden. Stevens en Koops komen in hun onderzoek (tot 2009) ten aanzien van kinderporno tot de conclusie dat dit verweer nergens wordt gehonoreerd.[359] Dat is in de periode daarna tot eind 2014 niet anders.[360]

---

[352] Het aantreffen van technieken op de computer van de verdachte (en in het civiel recht van de gedaagde) die downloaden alleen mogelijk maken als er ook wordt geupload zal er in de regel toe leiden dat het niet aannemelijker wordt dat de verdachte het bestand niet heeft geüpload.

[353] Of toegang had gegeven tot zijn of haar cloudopslag. Door wachtwoorden te delen kunnen enkele vrienden samen een heel grote collectie delen. Het verweer dat de verdachte het bestand nooit heeft aangeschaft is buiten beschouwing gelaten. Hoewel het niet ondenkbaar is, mede omdat er fouten gemaakt kunnen zijn in het watermerkproces, zal dit ook in het rapport worden besproken. Wanneer dit onvoldoende duidelijk is zal het OM het watermerk niet als bewijsmiddel gebruiken.

[354] Zie daarvoor Stevens en Koops 2009. Oerlemans bevestigt in zijn noot onder Hof 's-Gravenhage 18 januari 2013 BZ9494, CR 2013/161 dat de factoren anno 2013 nog niet lijken te zijn veranderd. Stevens en Koops 2009 noemen o.m. de computerkennis van de verdachte; aan- of afwezigheid van speciale programmatuur.

[355] Stevens en Koops 2009.

[356] Hoewel de jurisprudentie nog geen expliciete zaken kent waarin gebruik wordt gemaakt van bewijs uit de 'cloud' (zie tot 2012 ook Koops e.a. 2012) gelden daarvoor in beginsel dezelfde principes. Ook daar zal bijvoorbeeld gelden dat je moet aantonen aan wie je de wachtwoorden hebt gegeven dan wel aannemelijk maken dat je bent gehackt.

[357] Zie daarvoor o.m. Stevens en Koops 2009.

[358] Zie Haagman & Ghavatas 2005, p. 23-30; Bhoedjang 2008, p. 395; Stevens & Koops 2009, par. 2.2.3.

[359] Stevens en Koops 2009 (slot par. 2.2.3) merken op dat plaatsing door onbekende derden onaannemelijk is als elk hackerspoor ontbreekt dat forensisch deskundigen hadden moeten aantreffen en de verdachte bovendien zelf

De gerechten achten de verweren vaak ongeloofwaardig in het licht van andere vastgestelde feiten. Zo achtte de rechtbank het hack-verweer ongeloofwaardig nu het 'peer to peer'-programma (Gigatribe) waarvan bekend was dat daarmee kinderporno werd uitgewisseld, was geinstalleerd en een paar maanden later weer was verwijderd. Verdachte had daarnaast gebruik gemaakt van het chatprogramma van Gigatribe en verdachte had dit bekend. Bovendien was in de gebruikte Path naam de naam van de verdachte verwerkt en op de bij hem in beslag genomen USB-stick was onder meer het bestand 'deleted folder Gigatribe' aangetroffen.[361] Ook het Hof 's-Gravenhage achtte een dergelijk verweer niet aannemelijk omdat dit niet nader werd onderbouwd. Bovendien werd het niet ondersteund door het digitale onderzoek dat op de computers van verdachte was verricht en evenmin door de inhoud van de verklaringen van de getuigen. Daar komt nog bij dat uit onderzoek van de digitale recherche was gebleken dat via twee verschillende computers met de accounts was ingelogd en van beide accounts op beide computers ook nog eens een Hotmail-mailbox werd aangetroffen.[362]

Gerechten achten het verweer dat de verspreiding het gevolg is van een virus, ook vaak ongeloofwaardig.[363]

Een verdachte die voldoende aannemelijk maakt dat hij er alles aan heeft gedaan om te voorkomen dat de bestanden vanaf zijn computer konden worden geupload door bestanden altijd naar een aparte map te verplaatsten en de upload-functie van zijn downloadprogramma te minimaliseren, kan de rechter overtuigen dat er geen sprake is van (voorwaardelijke) opzettelijke verspreiding van kinderporno.[364] In de auteursrechtelijke E-donkey-zaak achtte de rechter het beperken van de (veelal) automatische upload functie van p2p-software weliswaar denkbaar maar niet aannemelijk wanneer dit ten koste gaat van de downloadsnelheid gelet op de werking van de verschillende systemen (software) en de intentie van gebruikers van P2P netwerken die erop is gericht om de bestanden zo snel en in zo groot mogelijk aantal te verkrijgen en verspreiden.[365]

Uit jurisprudentie blijkt dat forensisch onderzoekers, afhankelijk van de omstandigheden van het geval, in staat blijken om aan te tonen dat bestanden zijn geüpload.[366] Om binnen dat

anti-hackprogrammatuur heeft geïnstalleerd. Rb. Utrecht 1 december 2008, ECLI:NL:RBUTR:2008:BG5730. Zie voor verweren inzake kinderporno Stevens & Koops 2009.

[360] Oerlemans bevestigt in zijn noot onder Hof Den Haag 18 januari 2013, ECLI:NL:GHDHA:2013:BZ6496, CR 2013/161 m.nt. J.J. Oerlemans, dat de factoren anno 2013 nog niet lijken te zijn veranderd. Na onderzoek in de periode 1 januari 2009 - 31 december 2014 op de termen [hack, hacken] worden in het strafrecht 30 zaken gevonden en in geen van deze zaken is een verweer ten aanzien van een mogelijke hack gehonoreerd.

[361] Rb. Rotterdam 31 maart 2011, ECLI:NL:RBROT:2011:BP9776

[362] Hof Den Haag 30 september 2013, ECLI:NL:GHDHA:2013:3706.

[363] Onderzoek voor de periode 2009 - november 2014 levert met de zoektermen [virus, computer, kinderporno] 3 relevante resultaten waarbij de rechter het in het licht van het dossier onaannemelijk acht dat de kinderporno door middel van een virus is verkregen dan wel verspreid.

[364] Rb. Middelburg 2 december 2009, ECLI:NL:RBMID:2009:BL9868, ov. 4.3.

[365] Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey).

[366] Zie o.m. HR 09-10-2012, BX6949, NJ 2013, 62 m.nt. A.H. Klip; Hof 's-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010: BO8246, m.nt. Duker, AMI 2011/5, nr. 9, (e-donkey) geeft tevens een overzicht hoe een proces van verdenking tot huiszoeking loopt.

feitencomplex een succesvol derden-verweer te kunnen voeren zal de verdachte aansluiting moeten zoeken bij de onderzochte computer. Dat betekent dat hij zal moeten verklaren dat meerdere mensen toegang hebben tot zijn computer of dat hij zijn computer heeft uitgeleend.

Stevens en Koops kwamen ten aanzien van kinderporno al eerder tot de conclusie dat een dergelijk verweer meer kans van slagen heeft dan het hack-verweer.[367] De verdachte zal dan wel moeten verklaren wanneer en aan wie hij de computer heeft uitgeleend om deze verklaring te kunnen controleren.[368] Onder omstandigheden kan een verweer slagen, bijvoorbeeld wanneer de computer meerdere weken uit de macht van de verdachte is geweest en niet uit het dossier zou kunnen worden afgeleid wanneer de bestanden zijn geüpload.[369] Ook wanneer de verdachte erin slaagt de rechter te overtuigen van zijn onwetendheid ten aanzien van bepaalde wachtwoorden voor toegang tot bepaalde mappen, kan het verweer slagen.[370] Anders dan bij grote hoeveelheden kinderporno is het bij muziek-, film-, en fotobestanden niet onwaarschijnlijk dat kinderen in de leeftijd van 14 jaar dergelijke materialen down- en uploaden.[371]

Zo betwistte een (militaire) verdachte niet dat er kinderpornografische afbeeldingen op zijn laptop stonden, maar betwistte hij de opzet op het bezit van kinderporno door te stellen dat de afbeeldingen door een derde, buiten zijn weten, op zijn computer moesten zijn gezet. Hij wees daarbij op ‘een van de vele bezoekers van zijn woning, hetzij ‘via wifi’, een peer to peer programma als Gigatribe of een hack door iemand die fysiek niet bij zijn computer aanwezig was.’ De militaire kamer sloot deze alternatieven uit op basis van de bevindingen van een digitaal rechercheur in het licht van andere verklaringen. Zo kwam er maar een beperkt aantal vrienden over de vloer (twee à drie keer per maand), waren er een antivirusprogramma en firewall geïnstalleerd, en was er geen hackingsoftware aangetroffen.[372]

Ook in een witwaszaak achtte de rechtbank het hackverweer niet onmogelijk maar had zij geen enkele aanwijzing in het dossier aangetroffen welke in de richting van hacken wees, terwijl daar andere (verklaringen) tegenover stonden.[373]

Het enkel noemen van een naam is ook zonder nadere onderbouwing en in het licht van andere feiten onvoldoende om in het verweer te slagen.[374]

Verweren waarbij gewezen wordt op het per ongeluk laten open staan van mappen zullen in de regel ook niet snel worden gehonoreerd omdat rechters in kinderpornozaken erop wijzen

[367] Stevens & Koops 2009, par. 2.3.3.
[368] Rb. ’s-Hertogenbosch 24 december 2008, ECLI:NL:RBSHE:2008:BG9125.
[369] Rb. ’s-Gravenhage 4 december 2008, ECLI:NL:RBSGR:2008:BG6090 kon uit het dossier afleiden wanneer de bedoelde afbeeldingen op de harde schijf terecht waren gekomen.
[370] Rb. ’s-Hertogenbosch 29 oktober 2008, ECLI:NL:RBSHE:2008:BG3640.
[371] Rb. ’s-Gravenhage 31 juli 2006, ECLI:NL:RBSGR:2006:AY5348.
[372] Rb. Gelderland (militaire kamer) 2 september 2013, ECLI:NL:RBGEL:2013:2802, ov. 3.
[373] Rb. Utrecht 30 november 2010, ECLI:NL:RBUTR:2010:BO6823, ov. 4.3.
[374] Rb. Zwolle-Lelystad 16 september 2010, ECLI:NL:RBZLY:2010:BR4213

dat naar vaste jurisprudentie wordt aanvaard dat de verdachte die bestanden (met behulp van bestandsuitwisselingsprogramma) gedurende enige tijd in een (vrij toegankelijke) gedeelde map laat staan, de kans vergroot dat er meer mensen van kunnen kennisnemen en daarmee welbewust de aanmerkelijke kans aanvaardt dat bestanden worden verspreid.[375]

Evenals Stevens en Koops concluderen ten aanzien van kinderporno zal ook bij watermerken een verweer dat iemand anders de gewatermerkte bestanden heeft geüpload weinig kans van slagen hebben. Te meer als de verdachte niet kan aangeven wie en op welke wijze dat dan moet zijn gebeurd. A-G Machielse concludeerde voor HR 30 september 2008 in een strafzaak inzake kinderporno: 'Behoudens sterke aanwijzingen voor het tegendeel mag de rechter ervan uitgaan dat de daarop aangetroffen downloads zijn bewerkstelligd door de eigenaar van een laptop'.[376] Voor betrouwbare watermerken zouden dan gelden dat behoudens aanwijzingen voor het tegendeel de rechter er vanuit mag gaan dat het aangetroffen bestand is geüpload door de eigenaar van het bestand. Op basis van de huidige jurisprudentie lijkt mij dit zonder meer het uitgangspunt. Vooral in zaken waarin er geen andere sporen zijn dan digitale sporen en digitaal bewijs derhalve het enige bewijs is, is oplettendheid echter vereist. Anders dan in een zaak waarin DNA als bewijs wordt gebruikt is de bron bij digitaal bewijs fragiel en zijn digitale sporen vaak de enige sporen.[377] Dit terwijl digitale sporen perfect nagemaakt kunnen worden en tegenbewijs, mede vanwege de kosten, lastig te leveren kan zijn. Het ontbreken van hacksporen betekent niet dat er geen hack heeft plaatsgevonden. Onderzoek naar een hack is van verschillende factoren afhankelijk, zoals de kosten die met het onderzoek gepaard gaan maar ook de vraag hoeveel tijd er tussen de 'hack' en het onderzoek daarnaar zit. Soms worden er geen sporen gevonden, maar wordt de hack duidelijk omdat iemand erop een forum over opschept. In een zaak waarin één enkel bestand een rol speelt is waakzaamheid geboden. In veel zaken zal echter ook ander bewijs het verhaal compleet kunnen maken.

Samenvattend kan worden geconcludeerd dat ten aanzien van watermerken ook in het strafrecht drie typen verweren te voeren zijn: verweren die zich richten op de toelaatbaarheid, verweren die zich richten op de betrouwbaarheid en verweren die zich richten op een alternatieve verklaring voor het in beginsel bewezen feit. De eerste twee typen verweren raken direct de effectiviteit van het watermerk als bewijsmiddel. Het laatste type raakt weliswaar niet direct de effectiviteit maar zal voor met name voor de rechthebbende van belang zijn bij de vraag of hij watermerken wil inzetten als handhavingsmiddel. Een watermerk dat effectief is maar waarbij eenvoudig voorkomen kan worden dat er een verband kan worden gelegd tussen de licentienemer en het uploaden van het bestand, is voor de handhaving van het auteursrecht van weinig waarde. Het blijkt in de regel echter niet eenvoudig dergelijke verweren te voeren. De rechter acht de meeste verweren in het licht van

[375] Zie Rb. Dordrecht 10 augustus 2010, ECLI:NL:RBDOR:2010:BN3858. Rb. Amsterdam 3 juli 2009 ECLI:NL:RBAMS:2009:BJ8160 acht dit feit in 2009 nog geen feit van algemene bekendheid en kan mede na verklaring van een deskundige niet uitsluiten dat verdachte zich niet heeft gerealiseerd dat de door hem gebruikte programmatuur tijdens het downloaden van foto's/films ook het uploaden mogelijk maakt (o.v.3.3).
[376] Conclusie Machielse (ov. 6.5) voor HR 30 september 2008, ECLI:NL:HR:2008:BD4872.
[377] Par. 6.2.

het dossier veelal niet aannemelijk. Het enige verweer dat een kans maakt is dat de verdachte zijn computer heeft uitgeleend en kan aanwijzen aan wie. Voor het OM en de rechthebbende zal dat in de regel weinig uitmaken omdat zij daarmee een goed spoor hebben naar een andere verdachte dan wel gedaagde in een civiele procedure.

4.4.3 Beslissen over feiten: het bewijsoordeel

In beginsel is het onderzoek ter zitting de enige bron van informatie van de rechter. Alle informatie die kan leiden tot de bewezenverklaring moet zijn gebaseerd op het onderzoek op de terechtzitting.[378] De rechter mag daarbij alleen gebruik maken van in de wet erkende bewijsmiddelen. Hij is vrij in de selectie en waardering daarvan. In het bewijsminimum kunnen enige voorschriften met betrekking tot de bewijskracht worden gelezen. In beginsel geldt dat er altijd minimaal twee bewijsmiddelen nodig zijn om tot een bewezenverklaring te komen.[379] Daarbij geldt dat minimaal één bewijsmiddel de gehele bewezenverklaring moet dekken waarbij het vervolgens voldoende is wanneer een ander bewijsmiddel een (ondergeschikt) deel daarvan bevestigt.[380] Dat betekent dat het watermerk per definitie niet het enige bewijsmiddel kan vormen dat kan leiden tot een veroordeling van de verdachte. Voor het watermerk is van belang dat een verslag dat is opgesteld door een niet door de rechter aangestelde deskundige (deskundige rechthebbende) een schriftelijk bescheid vormt ex artikel 344 lid 1 onder 5° Sv dat in de categorie valt van zogenoemde ‘andere geschriften’ die alleen als bewijs kunnen gelden in verband met de inhoud van andere bewijsmiddelen.

Om tot een beslissing te kunnen komen zal de rechter moeten nagaan of hij vrij is in de waardering van het watermerk of dat er beperkingen zijn gesteld aan de waardering daarvan (par. 4.3.3.1). De rechter kan zich bij het waarderen van het watermerk te allen tijde laten voorlichten door een deskundige (par. 4.3.3.2).

4.4.3.1 Beslissen over watermerken

Het watermerk zal evenals in het civiele recht in de regel worden ingebracht in de vorm van een schriftelijk rapportage. De rechter is vrij in de waardering daarvan.

De wetgever heeft met de structurering van het onderzoek ter terechtzitting en met eisen van wettige bewijsmiddelen (art. 339 Sv), voorgeschreven bewijsminima (art. 352, lid 1 Sv) en de eis van de rechterlijke overtuiging (art. 338 Sv) beoogd de oordeelsvorming van de rechter te kanaliseren en te objectiveren. Hiermee heeft hij een stelsel in het leven willen roepen dat de rechter noodzakelijke ruimte biedt om tot een kwalitatief hoogwaardig en betrouwbaar

[378] Nijboer 2011, p. 65; Simmelink 2001, par. 2.1 onder d; Voor schriftelijke bescheiden, zoals rapportages, geldt hetzelfde, zij het dat dit niet verwoord is in art. 344 Sv, maar volgt uit art. 301, lid 5 Sv.
[379] Nijboer 2011, p. 77. Zie ook A-G Jorg (ov. 10) in zijn conclusie bij HR 21 november 2000, ECLI:NL:HR:2000:AA8408.
[380] HR 8 juni 1931, NJ 1932, p. 1550.

bewijsoordeel te komen.[381] De wetgever en daarmee het bewijsrecht gaan uit van een rechter die binnen de grenzen van het recht actief op zoek gaat naar de materiële waarheid.[382]

Elke bewijsbeslissing is inherent onzeker doordat alternatieven nooit honderd procent kunnen worden uitgesloten.[383] Wanneer absolute zekerheid niet mogelijk is rest de vraag hoeveel zekerheid voor de rechter nodig is om tot een positieve bewijsbeslissing te komen. In het strafrecht is de bewijswaarderingsmaatstaf opgenomen in artikel 338 Sv dat bepaalt dat door de rechter de overtuiging moet zijn bekomen, dat de verdachte het tenlastegelegde feit heeft begaan. In de literatuur is overeenstemming dat deze rechterlijke overtuiging neerkomt op een zeer klemmende graad van waarschijnlijkheid.[384] Het moet met andere woorden buiten redelijke twijfel staan dat de verdachte het tenlastegelegde feit heeft begaan.[385] In Common Law-stelsels spreekt men in dit verband ook van 'beyond reasonable doubt'.[386] Hiermee is duidelijk dat de bewijswaarderingsmaatstaf hoger ligt dan de redelijke mate van zekerheid in het civiel recht. Onduidelijk is of de strafrechter ook daadwerkelijk een hogere maatstaf aanlegt dan zijn civiele collega. De maatstaf blijft in de praktijk echter lastig te bepalen.

Cleiren illustreert en concludeert dat op basis van een beknopt overzicht van posities in de wet, de rechtswetenschappelijke literatuur en de rechtspraktijk er geen eenduidig antwoord kan worden gegeven op de functie en de inhoud van de rechterlijke overtuiging. Zij concludeert, mede in het licht van het bewijsrecht, dat de notie van de rechterlijke overtuiging een zwakke plek vormt met het oog op het benaderen van de historische werkelijkheid.[387] In het licht van de waarderingsmaatstaf en de motiveringsplicht is de persoonlijke overtuiging van de rechter, in het kader van de kwaliteit en de legitimiteit van de bewijsbeslissing, zeer beperkt. Cleiren ziet de functie van de overtuiging dan ook vooral in een opdracht aan de rechter om zich bewust te blijven van zijn rechterlijke verantwoordelijkheden in het kader van de waarheidsvinding (een inscherpingsfunctie, de referentie aan het geweten) die daarmee een overbrugging vormt tussen een feitelijk oordeel en een rechtsoordeel.[388] De overtuiging vormt daarbij tevens een maatstaf ter bevordering van het 'waarheidsgehalte' van de bewijsbeslissing door een bepaald niveau van waarschijnlijkheid te eisen (betrouwbaarheidsfunctie). In relatie tot de waarheid en een aanvaardbaar vonnis biedt de rechterlijke overtuiging de rechter tevens de mogelijkheid om zijn eigen persoonlijke 'praktische' wijsheid toe te passen

[381] Zie o.m. Nijboer 2011, p. 72; Cleiren 2010, p. 263; Groenhuijsen 2004 p. 151.
[382] Simmelink 2001, par. 2.1 onder b.
[383] Zie ook civiel recht. Voor het strafrecht zie o.m. Van Koppen (2011), die stelt dat alternatieven op grond van het bewijs (theoretisch) altijd mogelijk blijven.
[384] Nijboer 2011, p. 7. Met deze graad van waarschijnlijkheid wordt aangesloten op maatstaf 'beyond reasonable doubt' in common law-stelsels. Cleiren 2010, p. 261 en de daar aangehaalde literatuur.
[385] Zie ook Knigge (ov. 19) in zijn conclusie bij HR 2 februari 2010, ECLI:NL:HR:2010:BJ7266. Nijboer 2011, p. 73. Om de maatstaf extra kracht bij te zetten wordt in strafzaken met een hoge mate van bewijscomplexiteit ook de eis gesteld dat deze in eerste aanleg door de meervoudige kamer moeten worden behandeld. Vgl. art. 369 Sv; Nijboer 2011, p. 74.
[386] Zie hiervoor o.m. Anderson, Schum & Twining 2005, p. 242 en 243 en voor de verschillen in het Amerikaanse recht Van Stekelenburg 2009 (diss.), p. 12.
[387] Cleiren 2010, p. 267.
[388] Cleiren 2010, p. 267.

(complementaire functie). De rechterlijke overtuiging is in die zin in de woorden van Dreissen 'een noodzakelijke maar niet voldoende voorwaarde voor de juistheid van het feitenoordeel.'[389] De rechterlijke overtuiging blijft daarmee een sprong met hindernissen.[390] Wat overtuigend is, is daarmee ook persoonsgebonden.[391]

De rechter moet derhalve met een zeer klemmende graad van waarschijnlijkheid ervan overtuigd zijn dat de verdachte het tenlastegelegde feit heeft begaan (art. 338 Sv). Ten aanzien van de overige beslispunten van art. 348 en 350 Sv is volgens Nijboer en Enschedé niet één lijn te trekken ten aanzien van criteria voor het juist aannemen van feiten.[392] Daarover kan in het algemeen wel worden opgemerkt dat wanneer feiten of omstandigheden leiden naar een voor de verdachte gunstige einduitspraak, het voldoende is wanneer de rechter die feiten of omstandigheden aannemelijk acht. Deze gedachte moet vooral worden gezien vanuit het schuldbeginsel, 'in dubio pro reo'.[393] In het strafrecht vindt de verdachte ook hierin zijn bescherming.

4.4.3.2 Deskundigen

Deskundigen hebben de afgelopen jaren, mede in het licht van de gerechtelijke dwalingen, veelvuldig in de belangstelling gestaan. Dit heeft geresulteerd in zeer veel literatuur en initiatieven.[394] Voor watermerken is het vooral van belang te bestuderen in welke mate de rechter gebruik kan maken van een deskundige en welke kwaliteitseisen er worden gesteld aan de onderzoeker die het onderzoek uitvoert.

De rechter kan zich bij het vergaren van relevante kennis laten voorlichten door een deskundige.[395] In de praktijk worden vooral bij forensische onderzoeken deskundigen geraadpleegd, dat kan op de zitting maar ook schriftelijk doordat partijen een verslag of een reactie op een verslag aan het dossier toevoegen.[396] Ook partijen kunnen met betrekking tot de bewijsvoering of verwerping van het gepresenteerde bewijs gebruik maken van een deskundige. De taak van de deskundige ziet vooral op het uitvoeren van een opdracht tot het verstrekken van informatie over de stand van de kennis op zijn vakterrein of tot het verslag doen van zijn verrichtingen en conclusies op grond van een opdracht tot onderzoek aan een persoon of object.[397] Hij kan zijn verklaring op schrift stellen of hij kan mondeling zijn

[389] Dreissen 2007 (diss.), p. 378.
[390] Cleiren 2010, p. 267.
[391] Rassin 2010, p. 208.
[392] Nijboer 2011, p. 75; Ch. Enschede 1966, p. 512.
[393] Dit theoretische verband tussen de onschuldpresumptie en de bewijsstandaard 'beyond reasonable doubt' wordt wel bekritiseerd door Twining 1994, p. 205. Zie ook Nijboer 2011, p. 75.
[394] Zie het uitgebreide rapport van Keulen e.a. 2010.
[395] Corstens 2014, p. 696; Kooijmans 2010, p. 463.
[396] Zie voor het gebruik van deskundigen in digitaal forensisch onderzoek o.m. HR 30 oktober 2007, ECLI:NL:HR:2007:BA6569; Rb. Haarlem 27 januari 2012, ECLI:NL:RBHAA:2012:BW5210.
[397] MvT, p. 4. De deskundige verklaart het verslag naar waarheid, volledig en naar beste inzicht te hebben opgesteld. Het verslag is gebaseerd op wat zijn wetenschap en kennis hem leren omtrent datgene wat aan zijn oordeel onderworpen is (art. 51l lid 3 Sv).

verklaring komen uitleggen.[398] In beide gevallen kan het wettig bewijs vormen (art. 339, lid 1 Sv), zij het dat het in het eerste geval een schriftelijk bescheid (onder 5) vormt en in het tweede geval een mondelinge verklaring van een deskundige (onder 3). Met betrekking tot de bewijswaardering valt uit de rechtspraak en doctrine alleen af te leiden dat de verklaring of het verslag van een enkele deskundige niet toereikend is om tot bewezenverklaring over te gaan.[399] Indien de verdediging beargumenteerd en concreet duidelijk maakt dat de gebruikte methode niet betrouwbaar is, zal de rechter daar in zijn motivering aandacht aan moeten besteden. Het recht op tegenonderzoek bestaat volgens de Hoge Raad wel, maar dat betekent niet dat ook in alle gevallen het tegenonderzoek ook wordt vergoed.[400]

Wie deskundig is valt lastig te zeggen. De rechter kan in beginsel iedereen die hij deskundig acht beëdigen en horen. De Hoge Raad heeft in de loop der tijd wel een aantal algemene criteria geformuleerd.[401] Sinds 1 januari 2010 kan de rechter enige steun vinden in het Wetboek van Strafvordering.[402] Met de invoering van de Wet deskundige in strafzaken is de taak van de deskundige duidelijker in de wet verankerd en is er een landelijk openbaar deskundigenregister, het Nederlands Register Gerechtelijke Deskundigen (NRGD) opgezet.[403] De Wet Deskundige in strafzaken is gebaseerd op de drie belangrijkste pijlers waarop de kwaliteit en bruikbaarheid van deskundigenbewijs in het strafproces zijn gefundeerd:[404] het recht op tegenspraak in het voor- en eindonderzoek; kwaliteitseisen met betrekking tot deskundigen in het strafproces en de rol van de rechter in het voor- en eindonderzoek. Kwakman merkt op dat de rechter met deze wet wat meer greep heeft op het betrekken van deskundigen bij het strafrechtelijke eindonderzoek, maar dat de rechter ook daarvoor niet zelden de zitting schorste om de deskundige in de gelegenheid te stellen nader onderzoek te

[398] Zie daarover artikel 51l en 51 m Sv.
[399] Nijboer 2004, p. 19. Vgl. HR 21 november 2000, NJ 2001.
[400] HR 13 mei 1997, NJ 1997, 152. Dat laat vergoeding op grond van 591 Sv onverlet. Zie Nijboer 2011, p. 200 voor een vergelijking met het EHRM. Dat is niet anders in de nieuwe wet, al zijn de voorwaarden nu wel duidelijker (art. 51j lid 4 Sv). De verdachte die zelf een deskundige inschakelt zal deze zelf moeten betalen, maar kan deze natoekenning verrekend zien op grond van artikel 591 Sv. Zie ook Corstens 2014, p. 698.
[401] HR 27 januari 1998, NJ 1998, 404 (Schoenmakersarrest); HR 18 mei 1993, NJ 1993, 728; Nijboer 2011, p. 198.
[402] Eerste boek, titel IIIC: De deskundige (art. 51i-m). De Hoge Raad had eerder al een aantal algemene criteria geformuleerd; zie o.m. HR 27 januari 1998, NJ 1998, 404 (Schoenmakersarrest); HR 18 mei 1993, NJ 1993, 728; Nijboer 2011, p. 198. Het Nederlands Register Gerechtelijke Deskundigen (NRGD) heeft mede vanwege het beperkte toepassingsbereik van de Wet deskundige in strafzaken een beperkte waarde. Tevens vraagt men zich in de literatuur af of de echte deskundigen wel in het register (willen) worden opgenomen. Zie o.m WODC-rapport van Keulen e.a. 2010. Het nieuwe wettelijke stelsel met betrekking tot deskundigenbewijs in het strafproces is niet van toepassing op (zogeheten) 'technisch opsporingsonderzoek' wat het bereik van de wet aanzienlijk verkleint.
[403] De Wet deskundige in strafzaken wijzigt het Wetboek van Strafvordering ter verbetering van de regeling van de positie van de deskundige in het strafproces (Stb. 2009, 33; nr. 18632). Inwerkingtreding per 1 januari 2010 (Stb. 2009, 351). Voor achtergronden verwijs ik o.m. naar het Besluit van 18 juli 2009, houdende instelling van het Nederlands register gerechtelijk deskundigen en kwaliteitseisen aan deskundigen in strafzaken (Besluit register deskundige in strafzaken) (Stb. 2009, 330). (www.nrgd.nl). Voor meer beschouwingen over de wet en het register verwijs ik o.m naar het WODC-rapport van Keulen e.a. 2010; Nijboer 2011, p. 194; Kwakman 2011.
[404] Kwakman 2011 B, p. 2083.

verrichten alvorens hij wordt gehoord.[405] De rechter is ten aanzien van het onderzoek van de deskundige dus niet zo lijdelijk als de wet eerder deed vermoeden.

De wet stelt geen specifieke eisen aan deskundigen.[406] De wetgever heeft ervoor gekozen om in het Besluit Deskundigen in strafzaken een stelsel van basiskwaliteitseisen en gedragscodes te introduceren waaraan deskundigen moeten voldoen om voor registratie in aanmerking te komen.[407] De rechter kan in beginsel iedereen die hij deskundig acht beëdigen en horen, maar dient wel te motiveren wanneer hij een deskundige benoemt die niet in het register is opgenomen en dient deze deskundige te toetsen aan dezelfde kwaliteitseisen als zijn gesteld om geregistreerd te kunnen worden.[408]

Om geregistreerd te kunnen worden als deskundige beoordeelt het College gerechtelijk deskundigen of de expert:[409]
a. beschikt over voldoende kennis van en ervaring op het deskundigheidsgebied waarop de aanvraag betrekking heeft;
b. beschikt over voldoende kennis van en ervaring op het desbetreffende rechtsgebied en voldoende bekend is met de positie en de rol van de deskundige daarin;
c. in staat is de opdrachtgever inzicht te bieden in de vraag of en zo ja, in hoeverre de vraagstelling van de opdrachtgever voldoende helder en onderzoekbaar is om deze vanuit zijn specifieke deskundigheid te kunnen beantwoorden;
d. in staat is op basis van de vraagstelling volgens de daarvoor geldende maatstaven een onderzoeksplan op te stellen en uit te voeren;
e. in staat is onderzoeksmaterialen en -gegevens in een forensische context volgens de daarvoor geldende maatstaven te verzamelen, vast te leggen, te interpreteren en te beoordelen;
f. in staat is de geldende onderzoeksmethoden in een forensische context volgens de daarvoor geldende maatstaven toe te passen;
g. in staat is zowel schriftelijk als mondeling over de opdracht en elk ander relevant aspect van zijn deskundigheid gemotiveerd, controleerbaar en in voor de opdrachtgever begrijpelijke bewoordingen te rapporteren;
h. in staat is een opdracht te voltooien binnen de daarvoor gestelde of afgesproken termijn;
i. in staat is zijn werkzaamheden als deskundige onafhankelijk, onpartijdig, zorgvuldig, vakbekwaam en integer te verrichten.

In relatie tot de eerder genoemde pijlers biedt het register een indicatie voor kwaliteit. In de literatuur zijn de meningen verdeeld over de mate waarin het daadwerkelijk bijdraagt aan een

[405] Kwakman 2011 A.
[406] MvT, TK 31116, 2006-2007, p. 6.
[407] Zie art. 51k Sv waarin verwezen wordt naar het Besluit register deskundigen in strafzaken. De kwaliteitseisen zijn opgenomen in art. 12 van het Besluit. Via art. 13 lid 2 onder f committeert de deskundige zich aan de gedragscode van het College Gerechtelijk Deskundigen.
[408] Art. 51lid 2 Sv.
[409] In art. 3 van het Besluit wordt het College benoemd en in art. 12 staan de hiergenoemde kwaliteitseisen beschreven.

betere kwaliteit van onderzoek.[410] De gedeelde mening lijkt, zoals de voorzitter van het College Gerechtelijke Deskundigen John Coster van Voorhout het formuleerde: 'Kwaliteitsverbetering van de strafrechtelijke waarheidsvinding is niet alleen afhankelijk van (de deskundigheid van) deskundigen. Dat hangt af van veel meer factoren. Maar als het deskundigenregister er een steentje aan kan bijdragen, dan is dat al winst.'[411] Geen wetgever zal de rechter de benodigde flexibiliteit willen ontnemen bij het benoemen van een deskundige in zijn zoektocht naar de waarheid. Waarschijnlijk is de huidige formulering ook ongeveer het maximale wat aan eisen gesteld kan worden zonder andere belangen van betrouwbaarheid te raken. Niet in de laatste plaats omdat de wetenschap zich enorm snel ontwikkelt. Dat geldt zeker ook voor het domein van ICT waar wetenschappelijk forensisch onderzoek nog in de kinderschoenen staat vergeleken met DNA-bewijs.[412]

De wetgever heeft zijn best gedaan en de rechter met verschillende normen weer een stap geholpen. Het blijft niettemin de rechter die in het licht van het voortschrijdende inzicht van de wetenschap het register kritisch moet benaderen en zich niet moet verschuilen achter het register. Hij zal in individuele zaken zich steeds moeten blijven afvragen of de algemene kwalificaties van de deskundige voldoende zijn voor de specifieke vraag die een deskundige moet beantwoorden. Het is tot slot ook de rechter die moet toetsen of de gehanteerde methode de juiste is (omstreden of juist niet) en op de juiste wijze is toegepast. De waarborgen moeten met andere woorden niet enkel gevonden worden in het register maar ook in de twee andere zuilen van tegenspraak en de rol van de rechter. Want de zuilen dragen allen bij aan het bestaan van de tempel. De rol van de rechter is van groot belang. Toch laat onderzoek zien dat het voor rechters moeilijk is om deskundigenbijdragen goed te toetsen terwijl zij verplicht zijn tot een uitspraak in het geschil te komen.[413] Niet in de laatste plaats omdat zij gewoon niet over de benodigde kennis beschikken. In de praktijk volgt de rechter de ingebrachte rapportage wanneer de verdediging geen actieve bijdrage levert aan mogelijke verweren.[414] Rijnsburger & Malsch constateren dat uit de rechterlijke uitspraken niet blijkt dat er een stevige toets van de deskundigenbijdrage heeft plaatsgevonden. Het is weliswaar aan de rechter om het verslag te toetsen, maar van de verdediging mag zeker ook een bijdrage worden verwacht. Met een toenemende complexiteit in (digitaal) forensisch onderzoek en een toenemend belang zal in de toekomst vooral de vraag een rol gaan spelen wie het (kennelijk) nodige onderzoek gaat betalen. Met name die ontwikkeling zal van groot belang zijn voor de waarheidsvinding.

---

[410] Voor meer beschouwingen over de wet en het register verwijs ik o.m. naar het WODC-rapport van Keulen e.a. 2010; Nijboer 2011, p. 194; Kwakman 2011.
Zie voor het deskundigenregister in het strafrecht o.m. Nijboer 2011, p. 194; Derksen 2010.

[411] Citaat ontleend aan Kwakman 2011 die verwijst naar de uitzending van Nieuwsuur van 9 november 2010.

[412] Bij DNA is de standaardisering en protocollering veel verder doorontwikkeld. Toch moet er ook op worden gewezen dat DNA een totaal ander soort bewijs is waar in verband met de dynamiek van de bron (DNA vs computerbestand) en de ontwikkelingen in het veld standaardisering ook veel minder mogelijk is. Zie daarover ook par. 6.2. Zie ook par. 4.2.2. over de complexiteit van digitale forensische opsporing.

[413] Rijnsburger & Malsch 2013.

[414] Rijnsburger & Malsch 2013, p. 6; Franken 2012.

.

Voor watermerken is het in ieder geval van belang vast te stellen dat uiteindelijk de rechter, eventueel naast de onderzoeken die partijen inbrengen, gebruik kan maken van deskundigen om zich te laten voorlichten of bijstaan. Over de wijze waarop het watermerk kan worden gewaardeerd gaat hoofdstuk 6.

4.4.4 Tussenconclusie

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te beoordelen is het watermerk in de context van het Nederlandse strafrecht geplaatst. De effectiviteit van bewijsmiddelen wordt daar beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en de stellingen die over dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd.

Het uitgangspunt van het strafprocesrecht wordt gekenmerkt door het schuldbeginsel dat inhoudt dat de verdachte voor onschuldig wordt gehouden totdat zijn schuld rechtens is komen vast te staan. Het is dan ook aan het OM om de verdachte een strafbaar feit ten laste te leggen en deze tenlastelegging te bewijzen. Van de verdachte kan niet worden gevraagd om zijn onschuld te bewijzen en in die zin rust er dan ook geen bewijslast op de verdachte, noch draagt hij het bewijsrisico.

Uit onderzoek is gebleken dat wanneer de verdediging geen actieve bijdrage levert door het aanvoeren van mogelijke verweren, de rechter in de praktijk het ingebrachte deskundigenrapport van het OM volgt. De wetgever biedt de verdachte voldoende mogelijkheden tot contra-expertise en de verdachte doet er dan ook goed aan om hier om bovenstaande reden gebruik van te maken. Het werkt in die zin in het nadeel van de verdachte dat hij in beginsel zelf de kosten van dit onderzoek moet dragen. Wanneer het onderzoek in voldoende mate heeft bijgedragen aan kort gezegd de materiële waarheidsvinding dan is het mogelijk dat zijn kosten worden vergoed. Niettemin blijft het risico ten aanzien van de kosten bij aanvang en tijdens de procedure voornamelijk bij de verdachte liggen.

De gedaagde kan ten aanzien van het watermerk in het licht van het gestelde feit in beginsel drie verweren voeren. Ten aanzien van het watermerk kan hij verweren voeren die de toelaatbaarheid en/of betrouwbaarheid van het watermerk betwisten. Beide verweren raken direct de effectiviteit van het watermerk dat erin bestaat dat het gestelde feit kan worden vastgesteld. Ten aanzien van het gestelde feit kan de gedaagde de positie innemen dat er alternatieve verklaringen bestaan voor het openbaar worden van het bestand bijvoorbeeld doordat iemand anders dat heeft gedaan (meer- en vaartverweer). Dit laatste verweer raakt de effectiviteit van het watermerk niet. De rechter kan het feit dat het bestand aan de licentienemer toebehoort immers vaststellen. De verdachte voert hier verweer tegen het verband tussen het op internet aangetroffen bestand en zijn schuld. Het is immers aan het OM om te bewijzen dat het werk openbaar is gemaakt door de verdachte. Zonder die vaststelling is

er geen sprake van een strafbaar feit. De verdachte dient voor zijn stelling wel enige onderbouwing te geven. Hij hoeft geen bewijs aan te dragen van het tegendeel maar zal wel aannemelijk moeten maken dat de door hem gestelde situatie zich redelijkerwijs kan hebben voorgedaan. Een blote stelling zal de rechter niet overtuigen. Onderzoek laat zien dat dergelijke verweren alleen een kans van slagen hebben wanneer duidelijk is geworden dat de verdachte zijn computer of andere drager aan een ander heeft uitgeleend. Hij zal dan wel duidelijk moeten maken aan wie hij dat heeft gedaan. Voor het OM of de rechthebbende zal dat in termen van handhaving uiteindelijk weinig uitmaken omdat het OM dan een duidelijk spoor heeft naar de vermeende inbreukmaker. Dat wordt anders als uiteindelijk niemand kan worden aangesproken.

De rechter is bij gebrek aan wettelijke bepalingen ten aanzien van de waardering van watermerken vrij in de waardering ervan. Ook in de jurisprudentie zal de rechter geen steun vinden voor de waardering van watermerken. Het komt ervoor de strafrechter dan op aan om zelf tot een oordeel te komen eventueel met de hulp van een door hemzelf benoemde deskundige dan wel op basis van de door partijen ingebrachte verslagen, experts of andere materialen. In de praktijk is het echter maar de vraag of de strafrechter snel zelf een deskundige zal benoemen. Daarvoor zal tenminste de verdachte een goed verweer moeten hebben gevoerd.

4.5 Beslissen over feiten naar Belgisch strafrecht

Het Belgische strafrechtelijk bewijsrecht is beperkt geregeld in het Wetboek van Strafvordering en kent haar grondslagen vooral in de literatuur en jurisprudentie.[415]

Als uitgangspunt geldt ook naar Belgisch strafrecht dat het aan het Openbaar Ministerie (hierna: OM) is om de verdachte een strafbaar feit ten laste te leggen en om te bewijzen dat hij het tenlastegelegde feit heeft begaan.[416] Ook naar Belgisch strafrecht geldt het vermoeden van onschuld. Dat heeft evenals naar Nederlands strafrecht tot gevolg dat in geval van twijfel omtrent het bewijs van de schuld van de beklaagde aan de tenlastegelegde feiten, de rechter dit in het voordeel van de verdachte laat werken. Evenals naar Nederlands strafrecht is de strafrechter in België actief in het zoeken naar de juridische waarheid.[417]

Het vaststellen van feiten is aan de rechter overgelaten. Hij kan de feiten onderzoeken door bestudering van het dossier en het onderzoek op de terechtzitting. In België geldt in beginsel een vrij bewijsstelsel waardoor de rechter in beginsel alle toelaatbare en betrouwbare

[415] Verstraeten 2012, p. 964.
[416] Verstraeten 2012, p. 967. De burgerlijke partij kan zich met zijn vordering ook tot de strafrechter wenden. De regels van het strafprocesrecht zijn op die procedure van toepassing. Dat betekent dat de burgerlijke partij ook de bestanddelen van het misdrijf moet bewijzen en de toerekening daarvan aan de beklaagde. Zie Verstraeten 2012, p. 180; p. 967. Deze kwestie wordt niet afzonderlijk behandeld.
[417] Zie ook in rechtsvergelijkend perspectief met Nederland voor de rol van de rechter bij de waarheidsvinding in het strafrecht, uitgebreid de dissertatie van De Wolf 2010. Zie verder ook Verstraeten 2012, p. 983.

bewijsmiddelen voor het bewijs kan gebruiken.[418] Dat geldt ook ten aanzien van feitelijke vermoedens. Ten aanzien van feiten stelt de wet weinig nadere eisen. Evenals in het Nederlands procesrecht is het uiteindelijk aan de rechter om te beslissen of het tenlastegelegde feit kan worden bewezen.

Bij aanvang van de procedure is het aan het OM om te bewijzen dat de beklaagde kwaadwillig of bedrieglijk inbreuk heeft pleegd op het auteursrecht (art. 80 Aw).[419] Het watermerk dient in een dergelijke procedure als bewijs dat het bestand aan de licentienemer toebehoort.

De effectiviteit van watermerken wordt naar Belgisch strafrecht beoordeeld in het licht van de door het OM te bewijzen stelling dat het bestand aan de licentienemer toebehoort, en de argumenten die over dat feit en het watermerk door de beklaagde zijn aangevoerd dan wel door de rechter zijn betrokken bij zijn beoordeling. Evenals naar Nederlands strafrecht kan de beklaagde er naar Belgisch strafrecht voor kiezen om zich te beroepen op zijn zwijgrecht zonder dat de rechter daar direct de consequentie aan mag verbinden dat het feit kan worden vastgesteld. Ook in die gevallen is het de verantwoordelijkheid van de rechter om ook te kijken naar gegevens die ontlastend zijn voor de verdachte en op zoek te gaan naar de waarheid.[420]

Vanuit dit perspectief is het vooral zinvol om aandacht te besteden aan de vraag welke stellingen het OM moet en de verdachte redelijkerwijs kan aanvoeren over watermerken en op welke wijze de rechter deze stellingen moet beoordelen. Om die reden wordt eerst ingegaan op de vraag bij welke partij het bewijsrisico ligt wanneer de feiten onduidelijk blijven en hoe partijen hun stellingen kunnen onderbouwen (par. 4.5.1). Daarna wordt ingegaan op aannemelijke verweren die de verdachte kan voeren om het watermerk ineffectief maken (par. 4.5.2). Tot slot wordt gekeken naar de vraag hoe de rechter tot zijn bewijsoordeel komt (par. 4.5.3). De paragraaf wordt afgesloten met een tussenconclusie (par. 4.5.4).

4.5.1 Bewijsrisicoverdeling

Het uitgangspunt van het strafprocesrecht wordt evenals in Nederland gekenmerkt door het schuldbeginsel dat inhoudt dat de verdachte voor onschuldig wordt gehouden totdat zijn schuld rechtens is komen vast te staan (praesumptio innocentiae).[421] De beklaagde kan dan ook niet worden gevraagd om mee te werken aan het bewijs tegen hem.[422] In die zin rust er dan ook geen bewijslast op de beklaagde, noch draagt hij het bewijsrisico. Dit komt ook tot uiting in zijn procespositie die in zoverre vrij is dat hij zelf zijn inbreng kan bepalen. De beklaagde kan er met zijn beroep op zijn zwijgrecht voor kiezen een passieve houding aan te

[418] Verstraeten 2012, p. 977.
[419] Zie voor andere strafbare feiten par. 3.4.2.2.
[420] Zie o.m. Verstraeten 2012, p. 983.
[421] art 6 lid 2 EVRM, 14 lid 2 BUPO-verdrag.
[422] Verstraeten 2012, p. 967;

nemen. Van hem mag niet worden gevraagd de onjuistheid van een bestanddeel van het misdrijf te leveren.[423] Ook in die gevallen is het de verantwoordelijkheid van de rechter om ook te kijken naar gegevens die ontlastend zijn voor de verdachte.[424]

De beklaagde kan ook naar Belgisch strafrecht zelf invloed uitoefenen door verklaringen af te leggen en invloed uit oefenen op het verloop van het onderzoek op de terechtzitting door bijvoorbeeld het stellen van vragen, inbrengen van stukken en dagvaarden en inbrengen van deskundigen. Afhankelijk van de omstandigheden van het geval zal de beklaagde er veelal baat bij hebben om verweer te voeren om de rechter van zijn onschuld te overtuigen. Omdat de rechter vrij is in het gebruik van bewijsmiddelen kan de rechter ook rekening houden met de houding van de verdachte tijdens het proces. Dat risico zal voornamelijk intreden wanneer de verdachte weigert specifieke gegevens bekend te maken die in het domein van de verdachte liggen en waarvan het OM en de rechter anders geen kennis zouden hebben. De rechter mag echter niet vaststellen dat een relevant bewijselement bestond dat uitsluitsel kon geven over de toerekening van het misdrijf en de beklaagde veroordelen omdat het aan hem was dat element aan te brengen.[425] Met dat zwijgen neemt hij het risico dat die gegevens geen rol spelen bij de oordeelsvorming. Het niet voeren van verweren bijvoorbeeld ten aanzien van de toelaatbaarheid van bewijsmateriaal kan ook gevolgen hebben voor de omvang van het onderzoek en de inhoud van het vonnis, maar dat ontslaat de rechter niet van zijn ambtshalve opgelegde verantwoordelijkheid om ook aandacht te hebben voor deze mogelijke (niet aangevoerde) verweren. Anderzijds geldt dat de rechter een aanbod van de verdachte om bewijs aan te bieden niet zonder reden mag passeren. In de regel zal een verdachte er goed aan doen verweer te (laten) voeren zodat de rechter expliciet gewezen wordt op de mogelijke verweren.

De bewijslast- en risiscoverdeling in het strafrecht ligt op grond van de onschuldpresumptie (rechtsvermoeden van onschuld) bij de vervolgende partij: het OM of een burgerlijke partij.[426] Het is dan ook aan het OM om te bewijzen dat de verdachte kwaadwillig of bedrieglijk inbreuk heeft gepleegd op het auteursrecht. (art. 80 Aw).[427] Eerder werd al duidelijk dat het watermerk slechts kan bijdragen aan het bewijs dat het bestand aan de licentienemer (beklaagde) toebehoort. Zelfs met een toelaatbaar en betrouwbaar watermerk zal nader bewijs nodig zijn om te bewijzen dat de beklaagde (licentienemer) het bestand zelf op het internet heeft gezet en daarmee inbreuk heeft gepleegd op het auteursrecht.

4.5.2 Meest aannemelijke verweren

Ook naar Belgisch recht zijn in beginsel drie soorten (hoofd)verweren te voeren; toelaatbaarheidsverweren, betrouwbaarheidsverweren en verweren die een alternatieve

[423] Cass. 9 oktober 1990, A.C. 1990-91, 68.
[424] Zie o.m. Verstraeten 2012 p. 983.
[425] Cass. 24 maart 2010, P.10.0407.
[426] Cass. 11 december 1984, A.C. 1984-85, 277; art. 6 lid 2 EVRM; o.m. Verstraeten 2012, p. 965.
[427] Zie voor andere strafbare feiten par. 3.4.2.2.

verklaring geven ten aanzien van het gestelde feit. De eerste twee verweren raken direct de effectiviteit van het watermerk omdat de rechter zowel een ontoelaatbaar als een onbetrouwbaar watermerk uiteindelijk niet als juridisch bewijs zal accepteren. Het laatst genoemde verweer raakt het watermerk als bewijsmiddel in beginsel niet. Wanneer de rechter het feit kan vaststellen op grond of met behulp van het watermerk is het watermerk immers effectief te noemen. Toch zal de waarde van het watermerk als bewijs- en handhavingsmiddel sterk afnemen wanneer het in de praktijk eenvoudig blijkt om met een alternatieve verklaring te komen ten aanzien van het door het watermerk bewezen feit. In deze paragraaf zal vooral aandacht worden besteed aan dit laatste soort verweer. De eerste twee verweren worden vanwege hun directe belang voor de effectiviteit van het watermerk in de volgende twee hoofdstukken nader besproken.

Verweren die een alternatieve verklaring bieden voor het gestelde feit raken in beginsel het watermerk als bewijsmiddel niet. In veel gevallen bevestigt het de waarde van het watermerk omdat dergelijke verweren de toelaatbaarheid en betrouwbaarheid niet ter discussie stellen maar het gestelde feit als uitgangspunt nemen. Het watermerk is dan een effectief bewijsmiddel gebleken omdat daarmee het gestelde feit door de rechter kan worden vastgesteld. Een dergelijk verweer speelt wel een rol ten aanzien van het watermerk. Wanneer dergelijke verweren immers eenvoudig zijn in te roepen zal het watermerk zijn handhavingseffect ook missen. De rechthebbende kan met het watermerk dan immers wel bewijzen dat het gestelde feit zich heeft voorgedaan maar de vraag of beweerde schending van het auteursrecht de licentienemer aangerekend kan worden blijft daarmee onbeantwoord. Anders gezegd, wanneer dergelijke verweren eenvoudig zouden worden toegewezen mist ook een effectief watermerk uiteindelijk in de procedure zijn effect.

In België was het niet mogelijk om een vergelijkbaar jurisprudentie-onderzoek te verrichten zoals in Nederland.[428] Op basis van in de literatuur gepubliceerde uitspraken mag worden aangenomen dat het evenals in Nederland niet eenvoudig is een verweer te voeren dat een alternatieve verklaring geeft voor het gestelde feit. Ook in België geldt dat een dergelijk verweer moet worden onderbouwd en dat daarvoor in de regel een deskundige nodig zal zijn.

4.5.3 Beslissen over feiten: het bewijsoordeel

Om tot een beslissing te kunnen komen zal de rechter moeten nagaan of hij vrij is in de waardering van het watermerk of dat er beperkingen zijn gesteld aan de waardering daarvan (par. 4.5.3.1). De rechter kan zich bij het waarderen van het watermerk te allen tijde laten voorlichten door een deskundige (par. 4.5.3.2).

[428] Zie par. 4.4.2. In de periode tot november 2013 zijn erop de termen [auteursrecht, strafrecht] 19 zaken gevonden waarvan er 0 relevant bleken om te bepalen wanneer de rechter het uploaden van bestanden bewezen acht. Ook de termen [upload] en [hack] leverden geen resultaat op. De term [kinderporno] leverde 10 resultaten op maar geen daarvan was relevant om te kunnen onderzoeken of een mogelijk verweer dat ziet op een alternatieve verklaring kans van slagen heeft in de rechtszaal.

4.5.3.1 Beslissen over watermerken

De innerlijke overtuiging van de rechter wordt door Traest ook wel omschreven als het resultaat van de vrije bewijsbeslissing.[429] De schuld van de beklaagde wordt volgens het Hof van Cassatie beoordeeld naar de innerlijke overtuiging van de rechter wanneer hij de menselijke zekerheid heeft dat de beklaagde schuldig is aan het hem tenlastegelegde feit.[430]

De rechter is in het Belgische strafrecht volledig vrij bij het bepalen van de bewijswaarde van bewijselementen.[431] Dat betekent dat de rechter alle bewijselementen (behoudens de wettelijk voorgeschreven elementen) waaronder het deskundigenverslag, het verslag van een technisch raadsman van een beklaagde en het vaststellen van een snelheidsmeter voor voertuigen vrij kan waarderen.[432] Die vrijheid wordt niet aangetast als de rechter het verslag en de getuigenverklaring van een deskundige geloofwaardig acht, terwijl deze deskundige na het uitbrengen van het verslag als technisch raadsman van een der partijen is opgetreden.[433] Dit is niet anders wanneer men een beroep doet op het recht van verdediging of eerlijke behandeling in een zaak waarbij het verslag van het deskundigenonderzoek rechtmatig is overlegd en aan tegenspraak is onderworpen. Zelfs niet wanneer niet alle regels van het Gerechtelijk Wetboek inzake de tegenspraak van het deskundigenonderzoek zouden zijn nageleefd.[434] Dit betekent in de praktijk dat de rechter een grote mate van vrijheid toekomt.

Het is niet aannemelijk dat dit bij het watermerk anders is. Bij bewijselementen die niet met elkaar in overeenstemming zijn zal de rechter een keuze moeten maken ten aanzien van de elementen die hij doorslaggevend acht bij zijn besluitvorming.[435] Hij is ook niet gebonden aan een hiërarchie van bewijsmiddelen waardoor hij de bevindingen van een deskundige boven die van een getuige kan laten prevaleren.[436] De regelmatig ingewonnen bewijselementen mag hij echter niet uit de debatten weren.[437] De vaststelling van de geloofwaardigheid van de bewijselementen is onaantastbaar. Controle door het Hof van Cassatie is slechts mogelijk bij de toepassing van een wettelijk begrip bij de vraag of de rechter op wettelijke wijze kon besluiten tot de gevolgtrekking die hij er in rechte uit afleidt.[438] Aan het watermerk komt voor

[429] Traest 1992, nr. 794.
[430] Verstraeten 2005, p. 883; Cass. 10 november 1992, A.C. 1992, 726.
[431] Er wordt hierbij verwezen naar artikel 342 Sv. Verstraeten (2005, p. 874) wijst erop dat het hier enkel een voorziening betreft inzake het assissenhof.
[432] Cass. 29 mei 1984, A.C. 1984-85, 1274; Cass. 28 februari 1995, A.C. 1995, 117; Cass. 7 december, A.C. 1999, nr. 665, T. Strafrecht, 2000, 161. Zie voor de technisch raadsman van een beklaagde Cass. 21 februari 1984, A.C. 1983-84, 347. De technische raadsman is een partijdeskundige en daarmee een getuige à décharge. Hij legt geen eed af en heeft derhalve een andere status dan de deskundige die door de onderzoeksrechter is aangewezen. Voor de snelheidsmeter zie o.m. Cass. 24 december 1991, RW 1991-92, 1062, m.nt. M. De Swaef; Cass. 15 januari A.C. 1991-92, 246).
[433] Verstraeten 2010, p. 1020; Cass. 7 december, A.C. 1999-00, 665, T. Strafrecht, 2000, 161.
[434] Verstraeten 2010, p. 1020; Cass. 5 maart 2002, Verkeersrecht 2002, 185.
[435] Verstraeten 2010, p. 1020; Cass. 21 april 1999, A.C. 1999, 231.
[436] Verstraeten 2010, p. 1020; Cass. 18 december 1991, JLMB, 1992, 473.
[437] Verstraeten 2010, p. 1021; Cass, 22 juli 1981, A.C. 1980-81, 646.
[438] Verstraeten 2010, p. 1021; Zie o.m. Cass. 19 mei 1987 A.C. 1986-87, 544, RW 1987-88, 675, m.nt. Verstraeten; Cass. 26 oktober 1988, A.C. 1988-89, 115.

de feitenvaststelling geen bijzondere bewijswaarde toe. Dat is bijvoorbeeld wel het geval bij onbemande automatische camera's in geval van overtreding van de Wegenverkeerswet, bij gebrek aan een wettelijke grondslag en materiële vaststelling door de verbalisant die bij wet in een specifiek opdracht is voorzien.[439] Een wetswijziging is niet voor de hand liggend, omdat de inzet van watermerken niet door de overheid plaatsvindt.

4.5.3.2 Deskundigen

Deskundigen hebben ook in België de afgelopen jaren veelvuldig in de belangstelling gestaan.[440] Dit heeft geresulteerd in zeer veel literatuur en initiatieven.[441] In de Belgische en met name Vlaamse literatuur is veel kritiek op kort gezegd het gebrek aan wettelijke bepalingen voor deskundigenonderzoek in strafzaken.[442] In België wordt het deskundigenonderzoek in de Code de procédure pénale (CPP) (artt. 156-169) en slechts zeer beperkt in het Wetboek van Strafvordering (art. 43-44bis Sv) geregeld. Voor watermerken is het vooral van belang te bestuderen in welke mate de rechter gebruik kan maken van een deskundige en welke kwaliteitseisen er worden gesteld aan de onderzoeker die het onderzoek uitvoert.

Ook in België mag de rechter bij de waardering van het bewijs gebruik maken van deskundigen. Behalve aan de aanstelling van de deskundige en de eedaflegging zijn er geen nadere eisen gesteld. Ook niet aan de deskundige, zijn werkwijze of de waarde die de rechter aan het expertiseverslag mag of moet hechten. Deskundigen kunnen worden omschreven als zij 'die wegens hun kunde of beroep bekwaam geacht worden om de aard en de omstandigheden van de misdaad of het wanbedrijf te beoordelen'.[443] Het is aan de onderzoekende magistraat of iemand als deskundige kan worden aangemerkt, tenzij bij wet anders is bepaald, zoals bij artsen. Er is ook geen bescherming voor de titel gerechtsdeskundige.[444] Naast de deskundige die de rechter aanwijst, is er ruimte voor de technische raadsman die partijen voorlicht en bijstaat met zijn deskundigheid. In het strafrecht stellen Huybrechts en De Smet dat het lastig is om bekwame experts te vinden die binnen een

[439] Verstraeten 2005, p. 880; Cass. 4 januari 1994, RW 1993-1994, 1054, m.nt. A Vandeplas.
[440] Zie o.m. Handelingen (5-12) van de Belgische Senaat van donderdag 17 februari 2011, namiddagvergadering waar mondelinge vragen worden gesteld over de problemen op het vlak van de gerechtelijke expertise (nr. 5-37). Verder kan er nog op worden gewezen dat er een zekere waterscheiding tussen Wallonië (NICC) en Vlaanderen heerst (Leuven). Het Nationaal Instituut voor Criminalistiek en Criminologie (NICC) heeft de wettelijke taak om forensisch onderzoek te coördineren en uit te voeren. Daarnaast bestaat het Forensisch Instituut van de Katholieke Universiteit Leuven (Interfacultair Instituut voor Forensische Wetenschappen). Historisch is hiermee de forensische expertise versnipperd ondergebracht bij technische en wetenschappelijke politielaboratoria en andere ondersteunende diensten alsmede bij private en universitaire experts.
[441] Zie uitgebreid Bruggeman e.a. 2009; De Smet 2009, p. 219-226. Zie verder Kwakman 2010, p. 115. Zie voor een overzicht o.m. Keulen e.a. 2010, p. 113-151.
[442] Zie uitgebreid Bruggeman e.a. 2009; De , p. 113. De kritiek uit met name Vlaanderen kan mede worden verklaard uit de zekere waterscheiding tussen Wallonië (NICC) en Vlaanderen (Leuven). Zie voetnoot 968.
[443] Art. 43 Sv. Het betreft hier geen wettelijke definitie maar slechts een aanwijzing van iemand die de procureur des Konings zo nodig kan vergezellen. Zie o.m. De Smet 2010, p.77).
[444] De Smet (2010, p. 78) stelt dat deskundigen op lijsten komen omdat rechters hen betrouwbaar achten en niet omdat zij hun bekwaamheid eerst hebben bewezen.

redelijke termijn een verslag opstellen tegen de vergoedingen (erelonen) in strafzaken.[445] De Smet geeft aan dat het zwaartepunt in het strafproces ligt in de voorbereidende fase. Wanneer een partij niet aandringt op tegenspraak in deze fase dan wordt deze van doorslaggevend belang omdat deskundigen zelden op zitting komen en de aanstelling van een tegenexpert niet vaak voorkomt.[446] Niet onbelangrijk is dat wanneer een civiele partij haar eis tot schadevergoeding bij de strafrechter indient hij zijn proceswaarborgen (op tegenspraak) niet verliest. Het Grondwettelijk Hof (Arbitragehof) wil de expertise zoveel mogelijk door toepassing van het Gerechtelijk Wetboek laten verlopen (art. 962-991) tenzij deze onverenigbaar is met het strafproces(recht).[447] Volgens het Hof van Cassatie is de strafrechter vrij bij zijn beslissing over de inbreng van partijen aan het onderzoek. Een weigering daarvan leidt niet tot nietigheid.[448] De voorschriften uit het civiel recht vormen in het strafrecht dan slechts richtlijnen.[449]

Wanneer het deskundigenonderzoek alleen gebruikt kan worden voor de afhandeling van burgerlijke belangen dan moet de strafrechter ook de artikelen 973 en 978 Ger. W. toepassen en vindt het deskundigenonderzoek van rechtswege op tegenspraak plaats. Partijen moeten dan in staat worden gesteld om de expertise van deskundige bij te wonen en opmerkingen te maken ten aanzien van zijn voorlopig verslag.[450] De voorschriften uit het civiel recht vormen in het strafrecht dan verder slechts richtlijnen.[451]

Van Keulen e.a. hebben in 2010 een rechtsvergelijkend onderzoek uitgevoerd binnen de thema's van de Wet Deskundigen in het strafrecht: het recht op tegenspraak in het voor- en eindonderzoek; kwaliteitseisen met betrekking tot deskundigen in het strafproces en de rol van de rechter in het voor- en eindonderzoek.[452] Evenals naar Nederlands recht zal hier worden stilgestaan bij de vraag naar de kwaliteit van het onderzoek en in het bijzonder van het vaststellen van de onderzoeker.

In België bestaat sinds 1971 al een wet voor registratie van gerechtelijke deskundigen en bestaan er officiële en onofficiële lijsten bij rechtbanken.[453] Voor deze registratie gelden geen kwaliteitseisen waardoor er een wildgroei aan deskundigen is ontstaan. Het is ook niet

[445] De Smet 2010, p. 78; zie ook De Smet voor de verdere problemen die dat oplevert.
[446] De Smet 2010, p. 86.
[447] Arbitragehof 30 april 1997, BS 19 juni 1997. Zie ook art. 2 Ger. W. Het Hof laat zich verder niet uit in welke gevallen hiervan sprake is. Dit is bijvoorbeeld denkbaar in die gevallen dat in het civiele recht de verplichting geldt stukken te overleggen die in het strafrecht in strijd kunnen zijn met het zwijgrecht en het vermoeden van onschuld. Zie o.m. Allemeersch 2007, p. 348; Bruggeman e.a. 2009, p. 182. Laenens e.a. 2008, p. 591.
[448] Cass. 8 februari 2000, JLMB 2000, 625 m.nt. A. Sadzat; Cass. 12 april 2000, RW 2000-2001, 306, m.nt. De Smet. Het gaat hier over de vraag in welke mate de aangestelde deskundige zijn opdracht tegensprekelijk kan uitvoeren.
[449] De Smet 2010, p. 88.
[450] Cass. 8 februari 2000, JLMB 2000, 625 m.nt. A. Sadzat; Cass. 12 april 2000, RW 2000-2001, 306, m.nt. De Smet. Het gaat hier over de vraag in welke mate de aangestelde deskundige zijn opdracht tegensprekelijk kan uitvoeren.
[451] De Smet 2010, p. 88.
[452] Zie uitgebreid Kwakman 2010.
[453] Kwakman 2010, p. 131.

aannemelijk dat er binnen afzienbare tijd wetgeving komt die eisen gaat stellen aan de kwaliteit.[454] De rechter heeft in die zin alle vrijheid om te benoemen wie hij deskundig acht.[455] Kwakman constateert dat vaak hoge verwachtingen bestaan, die de deskundigen op de verschillende lijsten, maar zelden waar kunnen maken. Dillen wijst naast het gebrek aan kwaliteitseisen ook op de zeer lage lonen en het gebrek van de confrontatie met de bureaucratie en administratie.[456] Daarnaast wordt erop gewezen dat deze wijze van erkennen van deskundigen ertoe leidt dat de lijsten veelal bevolkt worden door mensen die carrière willen maken. Daardoor neemt het risico toe dat zij lippendiensten bewijzen die niet altijd overeenkomen met waarborgen rondom de waarheidsvinding. In de literatuur wordt er ook wel op gewezen dat tegenspraak in België veel eerder tot voordeel van de rijke verdachte leidt dan tot waarheidsvinding.[457] De materiële waarheidsvinding komt immers in het gedrang wanneer het OM of de onderzoeksrechter een ingewikkelde onderzoekopdracht verstrekt aan een deskundige die weliswaar op een lijst voorkomt, maar niet opgewassen is tegen de rijke verdachte die wel van hoog gekwalificeerde deskundigen gebruik kan maken.[458]

Voorstellen die in de literatuur worden gedaan komen overeen met kwaliteitscontrole zoals deze ook in Nederland is voorgesteld.[459] Kwakman constateert dan ook dat registratie van deskundigen alleen kan bijdragen tot kwaliteitsbevordering van forensisch onderzoek als deze registratie gepaard gaat met strenge kwaliteits- en betrouwbaarheidseisen, een gestructureerd accreditatiesysteem, gedragscodes, forensische bijscholing, toereikende honoraria die recht doen aan de tijdsinvestering en andere (rand)voorwaarden, zoals voldoende tijd, ondersteunende voorzieningen en ander faciliteiten.[460]

Voor watermerken, die zeer specialistische kennis vereisen, is het OM door een gebrek aan voldoende ‘eigen’ deskundigheid volledig afhankelijk van de rechthebbende. Dat is voor de rechthebbende die de rapportage aanlevert in beginsel geen probleem. Voor de verdachte vormt dat voornamelijk een probleem wanneer hij zelf niet over voldoende middelen beschikt verweer te voeren tegen het watermerk. Dat probleem kan zich ook voordoen bij verweren die zien op alternatieve verklaringen omdat voor de onderbouwing van dergelijke stellingen veelal forensisch IT-onderzoek is vereist.

[454] Idem.
[455] Alleen het vergelijkend DNA-onderzoek is in de wet opgenomen (art. 44ter en 90undecies Sv).
[456] Dillen 2009 (p. 203) wijst erop dat gerechtelijke deskundigen per uur vaak nog minder betaald krijgen dan een ongeschoolde arbeider. Of zoals Dillen het formuleert: ‘Men is psychiatrisch gestoord als men voor de prijs van een tweedehands Trabant een nieuwe Rolls Royce geleverd wil zien.’
[457] Zie ook Handelingen (5-12) van de Belgische Senaat van donderdag 17 februari 2011, namiddagvergadering.
[458] Daargelaten dat er ook goede deskundigen die bereid zijn om met weinig middelen Goliath te bestrijden.
[459] Zie o.m. De Smet (2009 p. 220) die wijst op controle, billijke vergoeding, onpartijdigheid, communicatie tussen de rechter en de deskundige, internationale bewijsvergaring en -uitwisseling en professionalisering door institutionalisering.
[460] Kwakman 2010, p. 149.

4.5.4 Tussenconclusie

Om de effectiviteit van het watermerk als juridisch bewijsmiddel te beoordelen is het watermerk in de context van het Belgische strafrecht geplaatst. De effectiviteit van bewijsmiddelen wordt ook in België beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en de stellingen die over dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd.

Het uitgangspunt van het strafprocesrecht wordt gekenmerkt door het schuldbeginsel dat inhoudt dat de verdachte voor onschuldig wordt gehouden totdat zijn schuld rechtens is komen vast te staan. Het is dan ook aan het OM om de verdachte een strafbaar feit ten laste te leggen en deze tenlastelegging te bewijzen. Van de verdachte kan niet worden gevraagd om zijn onschuld te bewijzen en in die zin rust er dan ook geen bewijslast op de verdachte, noch draagt hij het bewijsrisico.

Uit onderzoek naar het Nederlandse strafrecht is gebleken dat wanneer de verdediging geen actieve bijdrage levert door het aanvoeren van mogelijke verweren, de rechter in de praktijk het ingebrachte deskundigenrapport van het OM volgt. In België is niet duidelijk wat de rechter in deze gevallen doet. In de literatuur wordt erop gewezen dat de rechter en het OM gebruik moeten maken van deskundigen die in het register zijn opgenomen maar dat deze registers verder geen kwaliteitszorg kennen ten aanzien van de ingeschrevenen. Dit kan in sommige zaken tot gevolg hebben dat een rijke verdachte een betere expert kan inroepen dan de staat of de rechter. Dit is anders dan in Nederland waar de deskundigheid van het Nederlands Forensisch Instituut (NFI), waar de meeste onderzoeken vanuit de zijde van het OM worden verricht, buiten twijfel staat.

De wetgever biedt de verdachte voldoende mogelijkheden tot contra-expertise en de verdachte doet er dan ook goed aan om hier om bovenstaande reden gebruik van te maken. Het werkt in die zin in het nadeel van de verdachte dat hij in beginsel zelf de kosten van dit onderzoek moet dragen. Wanneer het onderzoek in voldoende mate heeft bijgedragen aan kort gezegd de materiële waarheidsvinding dan is het mogelijk dat zijn kosten worden vergoed. Niettemin blijft het risico ten aanzien van de kosten bij aanvang en tijdens de procedure voornamelijk bij de verdachte liggen.

De gedaagde kan ten aanzien van het watermerk in het licht van het gestelde feit in beginsel drie verweren voeren. Ten aanzien van het watermerk kan hij verweren voeren die de toelaatbaarheid en/of betrouwbaarheid van het watermerk betwisten. Beide verweren raken direct de effectiviteit van het watermerk dat erin bestaat dat het gestelde feit kan worden vastgesteld. Ten aanzien van het gestelde feit kan de gedaagde de positie innemen dat er alternatieve verklaringen bestaan voor het openbaar worden van het bestand bijvoorbeeld doordat iemand anders dat heeft gedaan (meer- en vaartverweer). Dit laatste verweer raakt de effectiviteit van het watermerk niet. De rechter kan het feit dat het bestand aan de

licentienemer toebehoort immers vaststellen. De verdachte voert hier verweer tegen het verband tussen het op internet aangetroffen bestand en zijn schuld. Het is immers aan het OM om te bewijzen dat het werk openbaar is gemaakt door de verdachte. Zonder die vaststelling is er geen sprake van een strafbaar feit. De verdachte dient voor zijn stelling wel enige onderbouwing te geven. Hij hoeft geen bewijs aan te dragen van het tegendeel maar zal wel aannemelijk moeten maken dat de door hem gestelde situatie zich redelijkerwijs kan hebben voorgedaan. Een blote stelling zal de rechter niet overtuigen.

De rechter is bij gebrek aan wettelijke bepalingen ten aanzien van de waardering van watermerken vrij in de waardering ervan. Ook in de jurisprudentie zal de rechter geen steun vinden voor de waardering van watermerken. Het komt ervoor de Belgische strafrechter dan op aan om zelf tot een oordeel te komen eventueel met de hulp van een door hemzelf benoemde deskundigen dan wel op basis van de door partijen ingebrachte verslagen, experts of andere materialen. In de praktijk is het echter maar de vraag of de strafrechter snel zelf een deskundige zal benoemen. Daarvoor zal tenminste de verdachte een goed verweer moeten hebben gevoerd.

4.6 Samenvatting en conclusie

In dit hoofdstuk is vanuit het bewijsrecht nader ingegaan op de vraag of het watermerk in een juridische procedure een effectief bewijsmiddel kan vormen voor het feit dat het bestand aan de licentienemer toebehoort. Om de effectiviteit van het watermerk als juridisch bewijsmiddel te kunnen beoordelen is het noodzakelijk om naast het materiële recht dat in hoofdstuk 3 is besproken, het watermerk in de context van het bewijsrecht te plaatsen. De effectiviteit van bewijsmiddelen wordt in het bewijsrecht beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en de stellingen die ten aanzien van dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd. Zowel naar Nederlands als Belgisch civiel recht en strafrecht wordt uiteindelijk in dat samenstel van regels bepaald in hoeverre het watermerk effectief is in relatie tot het te bewijzen feit dat het bestand bij de licentienemer hoort.

Vanuit dit perspectief is per land en rechtsgebied onderzocht welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren ten aanzien van dit feit en het watermerk als bewijsmiddel. Tevens is onderzocht hoe de rechter juridisch tot het bewijsoordeel ten aanzien van het feit en watermerk komt. Daartoe is per land en rechtsgebied ten eerste gekeken naar de vraag welke stellingen partijen kunnen en soms moeten aanvoeren en welke partij het risico draagt wanneer de feiten onduidelijk blijven. Ten tweede is gekeken naar de meest aannemelijke verweren die de wederpartij kan voeren tegen het watermerk en het feit waarvoor het watermerk als bewijsmiddel wordt ingezet. Ten derde is aandacht besteed aan de vraag hoe de rechter tot zijn bewijsoordeel komt en welke rol deskundigen daarbij spelen.

Bewijsrisicoverdeling

In beide landen en op beide rechtsgebieden geldt dat het aan de rechthebbende of het OM is om het feit dat het bestand aan de licentienemer toebehoort aan te voeren en zo nodig te bewijzen. Het risico dat het feit niet bewezen kan worden ligt in beide landen en op beide rechtsgebieden aan de zijde van de rechthebbende dan wel het OM. Om te voorkomen dat de rechter het door de rechthebbende gestelde feit vaststelt, geldt zowel naar Nederlands als Belgisch civiel recht dat de licentienemer (gedaagde) voldoende verweer moet voeren. De wetgevers in beide landen en op beide rechtsgebieden geven de gedaagde dan wel de verdachte hiertoe de mogelijkheid, onder meer door hem de mogelijkheden te geven tot contra-expertise.

Onderzoek in het Nederlandse strafrecht laat zien dat wanneer de verdediging geen actieve bijdrage levert door het aanvoeren van mogelijke verweren, de rechter in de praktijk het ingebrachte deskundigenrapport van het OM volgt. Daarbij moet worden opgemerkt dat die rapportages veelal afkomstig zijn van het Nederlands Forensisch Instituut waarmee de strafrechter in Nederland veel vaker werkt en waarin hij vertrouwen heeft. Onderzoek in het Nederlandse merkenrecht laat wel zien dat rechters onderzoek van experts van partijen meer wantrouwend benaderen wegens de schijn van partijdigheid. Ik acht het in beide landen niettemin aannemelijk dat ook rechters in civiele zaken de meer technische rapportages (DNA, watermerken) van (partij-)experts en door hen zelf benoemde deskundigen volgen.[461] Mede omdat het voor rechters lastig zal zijn om deze rapportages te weerleggen. Naar Belgisch strafrecht geldt mijns inziens hetzelfde. Daarbij moet wel worden opgemerkt dat het vertrouwen in deskundigen met name in de literatuur relatief laag is omdat er in België geen kwaliteitseisen aan deskundigen worden gesteld waardoor het vertrouwen dat de rechters in België hebben in de experts waarschijnlijk minder groot is. Dat wil overigens niet zeggen dat zij de deskundige niet volgen, omdat ook een deskundige die onder collega's als een matige onderzoeker beoordeeld wordt nog altijd meer van technische materie af zal weten dan de rechter zelf.

Om verweer te kunnen voeren zal de gedaagde of verdachte in de regel een beroep moeten doen op een expert. In theorie kan hij ook op basis van de literatuur verweer voeren, maar dat zal zonder enige kennis van watermerken lastig zijn omdat er over de meeste commerciële watermerksystemen niet wordt gepubliceerd. Ook wordt er niet meegedaan aan wedstrijden waarin de betrouwbaarheid van het watermerk door de deelnemers wordt getest. Hierdoor is het lastig om op basis van literatuur of andere openbare bronnen verweer te voeren tegen het specifiek in de procedure gebruikte watermerk. De inzet van een expert brengt andere vragen met zich mee. De gedaagde of verdachte zal immers kosten moeten maken voor het inschakelen van de expert. Hij neemt daarbij tevens het risico dat de expert hem geen

[461] In dit hoofdstuk is een onderscheid gemaak tussen de expert die voor en door partijen worden ingezet en de deskundige die door de rechter wordt benoemd. De term deskundige is voorbehouden aan de door de rechter benoemde deskundige.

informatie kan geven die hem helpt bij zijn verweer. Zowel in het civiel recht als in het strafrecht is het vervolgens maar de vraag of hij (een deel van) deze kosten vergoed krijgt. Met name in het civiele recht komt de licentienemer (gedaagde) dan voor de vraag te staan of een schikking voor hem niet goedkoper is. Het watermerk wordt daarmee naast een bewijsmiddel ook een strategisch middel. Wanneer de gedaagde van te voren weet dat hij verweer moet voeren en kosten moet gaan maken om voldoende verweer te kunnen voeren en bovendien in een IE-zaak veroordeeld kan worden tot een volledige proceskostenvergoeding, is het maar de vraag of hij het op een rechtszaak laat aankomen.

Aannemelijke verweren

Om te voorkomen dat de rechter uiteindelijk het feit dat het bestand aan de licentienemer toebehoort enkel vaststelt op basis van de feiten die door de rechthebbende of het OM zijn aangevoerd zal de licentienemer voldoende verweer moeten voeren. Deze verweren zullen zich dan ook primair richten op de te bewijzen stelling dat het bestand aan de licentienemer toebehoort, en de stellingen die de rechthebbende over dat feit en het watermerk heeft aangevoerd. Samenvattend kan worden geconcludeerd dat ten aanzien van watermerken drie typen verweren te voeren zijn: verweren die zich richten op de toelaatbaarheid, verweren die zich richten op de betrouwbaarheid en verweren die zich richten op een alternatieve verklaring voor het in beginsel bewezen feit. De eerste twee typen verweren raken direct de effectiviteit van het watermerk als bewijsmiddel. Het laatste type raakt weliswaar niet direct de effectiviteit maar zal voor met name de rechthebbende van belang zijn bij de vraag of hij watermerken wil inzetten als handhavingsmiddel. Een watermerk dat effectief is maar waarbij eenvoudig voorkomen kan worden dat er een verband kan worden gelegd tussen de licentienemer en het uploaden van het bestand, is voor de handhaving van het auteursrecht immers weinig waard.

In de regel zal het niet eenvoudig zijn om succesvol verweer te voeren door met alternatieve verklaringen te komen. Ten eerste geldt in beide landen in zowel het civiele recht als het strafrecht dat de gedaagde of verdachte tenminste aan de rechter duidelijk moet maken waar hij zijn verweer op baseert. De enkele mogelijkheid suggereren is onvoldoende. De gedaagde of verdachte zal in veel gevallen een deskundige nodig hebben om zijn argument kracht bij te zetten. Ten tweede zal het verhaal van de gedaagde of verdachte moeten passen in de context van de feiten die reeds zijn komen vast te staan. Dit beperkt de mogelijkheden die kunnen worden aangevoerd. In de onderzochte jurisprudentie komen deze verweren zeer beperkt voor. In het Nederlandse strafrecht heeft de verdachte de meeste kans dat een dergelijk verweer slaagt wanneer hij aannemelijk kan maken dat en aan wie hij zijn computer heeft uitgeleend. Voor de rechthebbende zal dat uiteindelijk weinig uitmaken omdat het OM in die gevallen met die informatie in beginsel voldoende aanknopingspunten heeft om een nieuwe vervolging te starten. De rechthebbende kan wanneer deze informatie hem bekend wordt ook een civielrechtelijke actie starten. In die zin maakt het voor de effectiviteit van het watermerk als handhavingsmiddel weinig uit wanneer dit verweer succesvol is.

Bewijsoordeel

Nadat partijen hun stellingen hebben gepresenteerd en zo nodig bewezen, komt de rechter in beide landen en op beide rechtsgebieden toe aan het beoordelen van het bewijs. De rechter blijkt ten aanzien van de waardering van het watermerk in beide landen en in beide rechtsgebieden uiteindelijk vrij in de waardering van het bewijs. In Nederland heeft De Bock in haar dissertatie recent de civielrechtelijke bewijswaarderingsmaatstaf aangescherpt door in het kader van de waarheidsvinding meer aandacht te vragen voor de alternatieve verklaring. Zij sluit hiermee aan bij de ontwikkeling in het strafrecht naar aanleiding van de eerder waargenomen rechterlijke dwalingen. Haar bewijswaarderingsmaatstaf biedt echter geen oplossing voor de vraag op welke wijze de rechter het bewijs moet beoordelen. Daarmee is de rechter dus nog steeds vrij om te bepalen of hij het watermerk betrouwbaar acht of niet en of hij op grond daarvan overtuigd is dat het bestand aan de licentienemer toebehoort.

Bij een gebrek aan jurisprudentie ten aanzien van het waarderen van watermerken is de rechter in beide landen en op beide rechtsgebieden geheel vrij in de waardering ervan. Hij kan voor het beoordelen van de betrouwbaarheid van het watermerk een deskundige benoemen om hem voor te lichten. In zowel Nederland als België geldt in het civiel recht in beginsel dat de rechter alleen een deskundige zal benoemen wanneer de stellingen van partijen daartoe aanleiding geven en het verschil van mening enkel door een deskundige kan worden beslecht. In de meeste gevallen zal de rechter een oordeel vellen op basis van de stukken die partijen in het geding hebben gebracht. In beginsel is dat in het strafrecht in beide landen niet anders, al heeft de rechter in het strafrecht wel meer dan in het civiel recht de taak om naar de materiële waarheid te zoeken. In beide landen geldt echter dat rechters op beide rechtsgebieden in de praktijk uit oogpunt van tijdsdruk, efficiënt gebruik van de kostbare tijd of onderzoeks-capaciteit andere legitieme afwegingen maken.

De rechter die een deskundige wenst te benoemen staat voor de uitdaging de juiste deskundige te vinden. De deskundige moet niet alleen beschikken over de juiste expertise ten aanzien van watermerken maar ook over de vaardigheden om zijn expertise om te zetten naar de forensische praktijk. De markt in het civiele recht is thans in beide landen nog vrij. Dat is anders in het strafrecht waar naar Nederlands en Belgisch recht een register bestaat waarin de rechter in beginsel zijn deskundige moet vinden. Een belangrijk verschil tussen beide landen is de kwaliteitszorg. Waar in Nederland sinds de invoering van de Wet deskundigen in strafzaken een heel systeem van kwaliteitsvereisten en uiteindelijk een heel systeem van kwaliteitszorg geldt, ontbreekt deze voor een belangrijk deel in België. In de literatuur is dan ook de meeste kritiek op het gebrek aan kwaliteitscontrole. Ondanks dat het aannemelijk is dat de rechter niet snel tot de benoeming van een deskundige overgaat, zullen in hoofdstuk 6 deze criteria van belang blijken. De hier genoemde criteria kunnen immers ook worden gebruikt bij het beoordelen van de kwaliteit van (partij-)experts en de door hen opgestelde rapportage.

5 De toelaatbaarheid van watermerken als juridisch bewijs

> 'But what's the use of formality? In many cases it's nonsense. […] An examining lawyer cannot be bounded by formality at every step. The work of investigation is, so to speak, a free art in its own way'.[1]

5.1 Inleiding

In het vorige hoofdstuk is duidelijk geworden dat de effectiviteit van het watermerk als bewijsmiddel kan worden aangetast door de toelaatbaarheid ervan te betwisten.[2] Wanneer de rechter tot het oordeel komt dat het watermerk van het bewijs moet worden uitgesloten kan niet meer worden gesproken over een effectief bewijsmiddel. Het uitsluiten van bewijs wordt in de literatuur in beide landen en in beide rechtsgebieden in beginsel onder omstandigheden mogelijk geacht, maar dit wordt in het kader van de waarheidsvinding en het recht op verdediging niet als de meest wenselijke uitkomst gezien. Duidelijk zal worden dat de rechter niet snel overgaat tot het uitsluiten van het bewijs. De effectiviteit van het watermerk kan verder nog worden beperkt wanneer de rechter tot het oordeel komt dat het watermerk als bewijsmiddel op een onrechtmatige wijze is verkregen, en als gevolg daarvan het watermerk niet uitsluit maar aan het onrechtmatig handelen een sanctie verbindt, bijvoorbeeld in de vorm van een schadevergoeding.

Om de toelaatbaarheid van het watermerk te kunnen beoordelen moet eerst worden vastgesteld of het watermerk als een juridisch bewijsmiddel kan worden gekwalificeerd (par. 5.2). Duidelijk zal worden dat de kwalificatie van het watermerk in de praktijk geen probleem vormt voor de toelaatbaarheid ervan als juridisch bewijsmiddel.

In de literatuur worden ten aanzien van de toelaatbaarheid van bewijs verder drie vragen centraal gesteld.[3] Ten eerste de vraag wanneer een bewijsmiddel als onrechtmatig bewijs kan worden aangemerkt (par. 5.3).[4] Ten tweede de vraag welke gevolgen aan onrechtmatigheid

---

[1] D. Dostojevksi, Crime and punishment, 1866, IV, V.

[2] Zowel naar Nederlands als Belgisch strafrecht geldt in beginsel dat de rechter de rechtmatigheid van het bewijs ook moet beoordelen indien de verdachte de toelaatbaarheid niet specifiek betwist.

[3] Naar Nederlands recht wordt er ten aanzien van de vraag of het bewijs onrechtmatig is verkregen alsmede de vraag of onrechtmatig verkregen bewijs moet worden uitgesloten gesproken over het leerstuk van onrechtmatig verkregen bewijs. Zie o.m. naar Nederlands civiel recht Kremer 1999 (diss.); Embregts 2003 (diss.), Asser 2013, p. 155 en naar Nederlands strafrecht o.m. Nijboer 2011, p. 62. Naar Belgisch recht wordt veeleer gesproken van het leerstuk van het ongeoorloofd bewijs. Zie naar Belgisch civiel recht o.m. Allemeersch & Schollen 2002; Van Gerven 2006, p. 65; Van Kildonck 2010, p. 180; Cattoir 2013, p. 540 en naar Belgisch strafrecht o.m. Verstraeten 2012.

[4] Deze vraag wordt in het civiele recht ook wel onderverdeeld in de onrechtmatige verkrijging door partijen, de rechter en de onrechtmatige openbaarmaking. De eerste categorie zal hierna verder centraal staan. Zie voor een nadere bespreking verder met name Embregts 2003, p. 45, Kremer 1999, p. 80-86. Zie ook voor Belgisch civiel recht ook Allemeersch & Schollen 2002. Bij onrechtmatige verkrijging door de rechter moet gedacht worden aan het schenden van wettelijke waarborgen (bv. deskundigenbericht), algemene beginselen, zoals die van een goede procesorde of hoor en wederhoor. Kremer (1999, p. 80-86) acht deze vorm een schijngestalte. Zie voor kritiek daarop Embregts 2003, p. 60. Verder kan ook het openbaar maken of het verstrekken van het bewijs onrechtmatig zijn, bijvoorbeeld om dat gehandeld is in strijd met het recht op privacy.

van bewijs moeten worden verbonden (par. 5.4).[5] Ten derde de vraag of het bewijsmiddel betrouwbaar is.[6] De vraag naar de betrouwbaarheid van het watermerk, zoals bij valse watermerken, hangt samen met de vraag naar de waardering van het watermerk en zal worden beantwoord in hoofdstuk 6.

In de Nederlandse literatuur en rechtspraktijk is lang geen scherp onderscheid gemaakt tussen de vraag naar de (on)rechtmatigheid van het bewijs en de toelaatbaarheid daarvan. Kremer en Embregts stelden destijds in hun proefschriften dat dit samen zou hangen met het idee dat het in de praktijk vooral gaat over de vraag wat de rechter met het bewijs doet.[7] In de periode na het verschijnen van deze proefschriften lijkt hier langzaam verandering in te zijn gekomen.[8] In de meest recente arresten van de Hoge Raad worden deze vragen terecht apart behandeld.[9] De vraag naar de (on)rechtmatigheid van de verkrijging van het bewijs dient naar mijn mening wél een zelfstandige beantwoording. Ten eerste is het niet ondenkbaar dat men na de onrechtmatigheidsvraag niet meer toekomt aan de vraag van de toelaatbaarheid.[10] Ten tweede vereist de transparantie dit. In dat kader kan ook worden verwezen naar de opmerking van De Waard die, in een administratief procesrechtelijke context, stelde dat het van groot belang is dat 'als een rechtsplicht is geschonden, ook benadrukt wordt dat dit het geval is'.[11] Ten derde is het voor de wijze van redeneren beter om de vraag naar de onrechtmatigheid eerst te beantwoorden. Hiermee wordt voorkomen dat er een neiging ontstaat om vanuit het gevolg terug te redeneren en daarmee het (on)rechtmatigheidsbegrip toe te schrijven naar de gewenste uitkomst.[12] Ten vierde vanwege het normerende effect dat uitgaat van het kwalificeren van de bewijsgaring als (on)rechtmatig.[13] Een oordeel over de (on)rechtmatigheid vormt daarmee niet alleen een oordeel in de betreffende zaak, maar kan ook een precedent scheppen voor volgende zaken. Het vormt daarmee een richtlijn voor het (toekomstig) handelen. Deze normen kunnen worden versterkt door aan de niet naleving daarvan een sanctie te verbinden, zoals het uitsluiten van bewijs, het toekennen van een schadevergoeding of door het verminderen van de toe te wijzen schadevergoeding of in het strafrecht, strafvermindering.

---

[5] Met uitzondering van proefschriften over dit onderwerp lijkt zowel in de Nederlandse als Belgische civielrechtelijke literatuur de vraag naar de uitsluiting meer centraal te staan dan de vraag naar de sanctie ervan.
[6] Embregts 2003 (diss.), p. 47; Kremer 1999 (diss.), p. 13.
[7] Zie o.m. Kremer 1999, p. 13; Embregts 2003, p. 45.
[8] Zie o.m. Embregts 2003 (diss.), p. 48 en Kremer 1999 (diss.), p. 13. Van Stekelenburg 2009 (diss.), p. 47-49 passeert de vraag naar de toelaatbaarheid in zijn dissertatie over elektronische gegevens als bewijsmiddel.
[9] Zie eerst het Hof 's-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465 (Achmea/Rijnberg), ov. 34-35 en in cassatie HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.2.2-5.2.3; HR 11 juli 2014 ECLI:NL:HR:2014:1632, ov. 3.5, alsmede het Parket bij de Hoge Raad in conclusies voor beide arresten. Zie bijv. A-G Wissink (ECLI:NL:PHR:2014:489, ov. 2.12) voor HR 11 juli 2014, ECLI:NL:HR:2014: 1632, die stelt dat 'wanneer een partij klaagt dat door haar wederpartij ingebracht bewijs jegens haar onrechtmatig is verkregen, [...] de civiele rechter zich twee vragen [zal] moeten stellen a) is het bewijs inderdaad onrechtmatig verkregen en, zo ja, b) mag het bewijs al dan niet worden gebruikt?'.
[10] Zie ook Rachlinski (op p. 217) die erop wijst dat onderzoeken suggereren dat het voor rechters een serieus probleem is als zij zowel moeten beslissen over de toelaatbaarheid van het bewijs als over de uitkomst van de zaak.
[11] De Waard 1987, p. 310.
[12] Zie o.m. Kremer 1999, p, 13; Embregts 2003, p. 48.
[13] Zie Embregst 2003, p. 49 en de daar aangehaalde literatuur.

De vraag naar de onrechtmatigheid van het watermerk als bewijsmiddel (par. 5.3) en de vraag naar gevolgen die een eventuele onrechtmatigheid moet hebben voor het watermerk als bewijsmiddel (par. 5.4) worden dan ook apart behandeld.

Tot slot kan er nog op worden gewezen dat onderzoeken in de Verenigde Staten duidelijk maken dat rechters weliswaar pogingen doen om geen acht te slaan op relevant bewijs dat ontoelaatbaar is, maar er niet altijd in slagen zich niet door dit bewijs te laten beïnvloeden.[14] Dit gold ook in die gevallen waarbij duidelijk was dat het ontoelaatbaar bewijs betrof.[15] Rachlinski wijst erop dat deze onderzoeken suggereren dat het voor rechters een serieus probleem is als zij zowel moeten beslissen over de toelaatbaarheid van het bewijs als over de uitkomst van de zaak.[16] Dit komt niet onlogisch voor en zou ook voor de Nederlandse en Belgische praktijk kunnen gelden. Voor watermerken als bewijsmiddel betekent dit dat de presentatie van die resultaten ook van belang is wanneer deze ontoelaatbaar zijn, maar dezelfde rechter het vonnis wijst. Hoewel de toelaatbaarheid van bewijs zowel in Nederland, België als de Verenigde Staten formeel een rol speelt laten deze onderzoeken zien dat ondanks een eventuele ontoelaatbaarheid van bewijs, dergelijk bewijs toch van invloed kan zijn op de eindbeslissing.[17] Dit hoofdstuk richt zich verder op de juridische toelaatbaarheid van bewijs.

5.2 De kwalificatie van watermerken als juridisch bewijsmiddel

Om als bewijs te kunnen dienen zal het watermerk als een juridisch bewijsmiddel gekwalificeerd moeten worden. Omdat de kwalificatie als bewijsmiddel wel relevant is, maar in de praktijk nauwelijks tot problemen leidt, zal in de onderstaande paragraaf de kwalificatie van het watermerk als juridisch bewijsmiddel slechts kort worden besproken.

5.2.1 Civielrechtelijke kwalificatie

5.2.1.1 Nederland

In het Nederlandse civiele recht geldt de zogenoemde vrije bewijsleer, die mede tot uitdrukking komt in artikel 152 Rv. Tenzij de wet anders bepaalt, kan bewijs worden geleverd door alle middelen en is de waardering van het bewijs aan het oordeel van de rechter overgelaten.

Uit de parlementaire behandeling van het bewijsrecht blijkt dat voor watermerken, evenals voor andere ‘moderne’ bewijsmiddelen, de gangbare processuele voorschriften, voor zover

[14] Zie o.m. Rachlinski 2012, p. 27 en de daar aangehaalde literatuur. In deze onderzoeken stond de betrouwbaarheid van het bewijs niet ter discussie.
[15] Wistrich, Guthrie & Rachlinski 2005.
[16] Rachlinski 2012.
[17] De vragen die dit oproept ten aanzien van de wijze waarop in de rechtspraak wordt omgegaan met bewijs dat ontoelaatbaar wordt geacht is verder buiten beschouwing gelaten.

deze zich hier voor lenen, rechtstreeks dan wel naar analogie dienen te worden toegepast.[18] Het staat partijen op basis van artikel 152 lid 1 Rv dan ook vrij om een watermerk als een bewijsmiddel tijdig en op juiste wijze in het geding te brengen.[19] De vraag of het watermerk als een wettig bewijsmiddel kan worden gekwalificeerd zal zowel in de literatuur als in de rechtspraak, om hierboven genoemde redenen niet ter discussie staan.

Asser merkt op dat elektronische bewijsmiddelen wel een eigen plaats in het recht hebben omdat zij naar hun aard kunnen worden onderscheiden van het geschrift dat klassiek als het meest algemene bewijsmiddel geldt.[20] De voornaamste uitdaging ligt dan ook in de waardering van elektronische gegevens. Doordat tegenwoordig 'iedereen' eenvoudig toegang heeft tot verschillende software programma's waarmee elektronische gegevens kunnen worden geproduceerd en gemanipuleerd, speelt de vraag naar de betrouwbaarheid van elektronisch bewijs een belangrijke rol. Met name de authenticiteit (herkomst) en integriteit (inhoud) van elektronische informatie speelt daarbij een grotere rol dan bij geschriften. Van Stekelenburg vindt het opmerkelijk dat 'de authenticiteit van objecten of gegevens weinig aandacht krijgt in de [civiele] rechtspraak, juist omdat deze ook vaak zo eenvoudig te vervalsen zijn'.[21]

In het Nederlandse civiele recht is er derhalve geen reden om aan te nemen dat het watermerk niet als een wettelijk bewijsmiddel kan worden geaccepteerd. De grootste uitdaging is dan ook niet zozeer of het watermerk als wettelijk bewijsmiddel kan worden gekwalificeerd maar op welke wijze het moet worden gewaardeerd (hoofdstuk 6). Voor de toelaatbaarheid van het watermerk als bewijsmiddel is het vervolgens de vraag of het watermerk op andere wijzen ontoelaatbaar kan worden geacht.

5.2.1.2 België

Voor een antwoord op de vraag of het watermerk als middel tot bewijs kan worden toegelaten moet naar Belgisch recht eerst onderscheid gemaakt worden naar de aard van het geschil.[22] In commerciële of handelszaken geldt er met betrekking tot bewijsstukken zoals het watermerk, een zogenaamde vrije bewijsregeling (art. 25 Wkh).[23] Nu er in de wet verder geen beletsels zijn opgenomen waardoor het watermerk niet als bewijsmiddel kan worden beschouwd kan

[18] Parl. Gesch, Nieuw bewijsrecht, p. 104-109; zie verder o.m. Van Stekelenburg 2009 (diss.), p. 48; Asser 2013, p. 285.
[19] Zie ook art. 152 lid 2 Rv en Parl. Gesch. Nieuw bewijsrecht, p. 135.
[20] Asser 2013, p. 168. Zie o.m. de regelingen voor de elektronische handtekening (art. 3:15a BW), de langs elektronische weg tot stand gekomen overeenkomst (art. 6:227a BW) en de elektronische akte (art. 156 Rv). In beginsel is een onderscheid van weinig belang omdat de rechter behoudens de wettelijke beperkingen geheel vrij is in de waardering van het bewijs.
[21] Van Stekelenburg 2009 (diss.), p. 210. Kessler (2010 diss.) kwam tot dezelfde conclusie in zijn onderzoek ten aanzien van het gebruik van elektronisch bewijs in de Verenigde Staten.
[22] Cass. 17 juni 1983, A.C. 1982-83, 1290; zie ook Laenens e.a. 2012, p. 536.
[23] Er zijn wel wettelijke vermoedens opgesteld voor andere zaken zoals facturen.

het in een procedure tussen een rechthebbende en een handelaar, evenals naar Nederlands recht, eenvoudig als bewijsmiddel worden gekwalificeerd.

In een procedure met een niet-handelaar (consument) zal de rechthebbende in beginsel moeten nagaan of het watermerk in het wettelijk stelsel past van (gesloten) bewijsmiddelen zoals neergelegd in Burgerlijk Wetboek (BW) en het Gerechtelijk Wetboek (Ger. W).[24] In het burgerlijk recht wordt een aantal bewijsstukken als bewijsmiddel erkend: schriftelijk bewijs (art. 1317 e.v. BW; artt. 883 e.v. en 895 e.v. Ger. W.), getuigenbewijs (art. 1341 e.v. BW; artt. 915-961 Ger.W.), bewijsvermoedens (art. 1349 e.v. BW), bekentenis (art. 1354 e.v. BW) en de eed (art. 1357 e.v. BW; art. 1005 e.v. Ger. W.). In het Gerechtelijk Wetboek zijn verder nog enkele regelingen opgenomen met betrekking tot onderzoeksmaatregelen, zoals het proces-verbaal van vaststelling van materiële feiten door een gerechtsdeurwaarder (art. 516 Ger.W.), ambtshalve bevolen deskundigenonderzoek (art. 962-991 Ger. W) of het verhoor van partijen (art. 992-1004 Ger. W.). In dit gesloten stelsel is in beginsel geen ruimte voor nieuwe technologische ontwikkelingen, anders dan bij nieuwe wetgeving.[25] Dit heeft als voordeel dat er meer rechtszekerheid wordt geboden en dat de bewijsprocedure vereenvoudigd wordt.[26] Deze regeling wordt door sommige auteurs echter ook als onrechtvaardig en log gezien.[27] Door soepele interpretatie van basisbegrippen vinden nieuwe technologische ontwikkelingen vaak toch een weg in de rechtspraktijk, zolang zij geen afbreuk doen aan het recht op tegenspraak.[28] Het gesloten bewijs geldt in België volgens de regels van het Burgerlijk Wetboek enkel voor het bewijs van rechtshandelingen en niet voor het bewijs van feiten. Nu het watermerk in de vorm van een rapportage zal worden ingebracht als bewijs voor een feit zal het ook in burgerlijke zaken als bewijsmiddel kunnen worden gekwalificeerd en een verdere beoordeling door de rechter niet in de weg staan. Ook naar Belgisch recht zal de betrouwbaarheid van watermerken een grotere uitdaging vormen dan de kwalificatie daarvan als bewijsmiddel.

5.2.2 Strafrechtelijke kwalificatie

5.2.2.1 Nederland

In het Nederlandse strafrecht mag de rechter de bewezenverklaring alleen baseren op een gesloten stelsel van wettige bewijsmiddelen.[29] De wettige bewijsmiddelen zijn opgenomen in artikel 339, lid 1 Sv en worden gevormd door de eigen waarneming van de rechter,

[24] Zie ook Hof van Beroep Antwerpen 16 november 2009, NjW 2010, 545; Laenens e.a. 2012, p. 549; Cattoir 2013, p. 20..
[25] Cattoir 2013, p. 15, 243. Zie bijvoorbeeld de Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten (BS van 29.09.2001).
[26] Zie o.m. Laenens 2004, p. 276; Van Gerven 2006, p. 412; Laenens e.a 2012, p. 536.
[27] Zie o.m. Laenens 2004, p. 288; Van Compernolle 2002, p. 151; Laenens 2012, p. 536.
[28] Zie o.m. Cattoir 2013, p. 16, 151; Laenens e.a. 2012, p. 536; Van Gerven 2006, p. 696; Van Ommeslaghe 2004, p. 300-302. De strakke bewijs regels worden anderzijds weer soepel toegepast. Zie o.m de medewerkingsplicht van partijen.
[29] Art. 338, lid 1 Sv.

verklaringen van de verdachte, getuige of deskundige en schriftelijke bescheiden. Deze opsomming is noch limitatief noch is er in de praktijk sprake van een strikte scheiding tussen de verschillende bewijsmiddelen.[30] In Nederland is ook wel gepleit om het stelsel open te maken.[31] Nieuwe, niet opgesomde, bewijsmiddelen kunnen via de rechterlijke waarneming als wettig bewijs dienen, maar vormen niet zelfstandig een bewijsmiddel.[32] Hoewel het watermerk als bewijsmiddel nieuw is zal het in de regel in de vorm van een verslag worden ingebracht en gelden als een schriftelijk bescheid in de vorm van een rapportage (art. 344 lid 1 onder 5 Sv). Daarnaast kan een deskundige op verzoek van de rechter of partijen een verklaring afleggen over zijn wetenschap omtrent hetgeen aan zijn oordeel is onderworpen. De deskundige kan worden gevraagd de rechter en procesdeelnemers voor te lichten, bij te staan, onderzoek in stellen en waar dat uit zijn taak voortvloeit verslag uit de brengen.[33] Ook verslagen van deskundigen gelden als een schriftelijk bescheid. Zo kan de deskundige zowel ter zitting getuigen als via zijn verslag. Tot slot kan de eigen waarneming van de rechter van belang zijn wanneer het watermerk niet door bescheiden of door de verklaring van een deskundige tot een bewezenverklaring kan leiden.
Daarbij geldt vanzelfsprekend dat de wettelijke vormen in acht genomen moeten worden. Ook in het Nederlandse strafrecht geldt dat de betrouwbaarheid van het watermerk een grotere uitdaging zal zijn dan de positief te beantwoorden vraag of het watermerk als een wettig bewijsmiddel gekwalificeerd worden.

5.2.2.2 België

In tegenstelling tot het Nederlandse strafprocesrecht wordt het Belgische strafprocesrecht in beginsel gekenmerkt door het beginsel van vrije (tegen)bewijslevering (art. 342 W. Sv).[34] Dit uitgangspunt geldt voor zover de wet niet op een beperkende wijze een bijzonder bewijsmiddel voorschrijft.[35] Daarvan is overigens zelden sprake. Ook artikel 154 Wetboek van Strafvordering (Sv), waarin is opgenomen dat ‘overtredingen worden bewezen hetzij door processen-verbaal of verslagen, hetzij door getuigen bij ontstentenis van verslagen en processen-verbaal of tot staving ervan’ geldt niet als een dwingende beperking.[36] Hetzelfde

[30] Corstens 2014, p. 762; Nijboer 2011, p. 175.
[31] Zie o.m. Groenhuijsen 2001 (project strafvordering), laatste deel. Zie voor kritiek daarop o.m. Mevis e.d.
[32] HR 15 september 1980, NJ 1981, 13; HR 8 januari 2002, ECLI:NL:HR:2002:AD5594, NJ 2002, 340 m.nt. Sch; HR 31 oktober 2006, ECLI:NL:PHR:2006:AX9179 en HR 15 december 2009, ECLI:NL:HR:2009:BK2129 NJ 2010, 26. Nijboer 2011, p. 176-177 noemt het bewijsmiddel van de eigen waarneming van de rechter in het licht van artikel 344 lid 1, sub 1-4 Sv een restcategorie. Zie ook HR 8 mei 2001, ECLI:NL:HR:2001:AB1517, NJ 2001 479, met name A-G Fokkens voor dit arrest (ov. 22).
[33] Zie de artt. 51i e.v., 227 en 229 Sv. Zie ook Nijboer 2011, p. 195.
[34] Zie o.m. Verstraeten 2012, p. 977, 1018.
[35] Zie o.m. Verstraeten 2012, p. 977; Cass. 26 maart 2001, A.C. 1990-91, 400; Cass. 20 december 2000, A.C. 2000, 714.
[36] Verstraeten 2012, p. 978; zie o.m. Cass. 19 juni 1990, A.C. 1989-90, 609; Cass. 26 november 2008, RW 2010-11 rijden onder invloed niet enkel door bloedanalyse; Rb. Gent, 6 februari 1992, TGR 1992, 65 voor het gebruik van videobanden; Cass. 4 juni 2008, P.08.0489.F ten aanzien van algemene ervaringsregels.

geldt wanneer de wet bij bepaalde misdrijven specifieke of bijzondere bewijsmiddelen vooropstelt, ook dan kan bewijs via ander bewijs worden geleverd.[37]

Voor inbreuk op het auteursrecht zijn geen specifieke of bijzondere bewijsmiddelen vooropgesteld. Het bewijs inzake inbreuk op het auteursrecht kan dan ook vrij worden geleverd. In de literatuur worden in het algemeen het proces-verbaal, bekentenissen, verklaringen van partijen en getuigen, feitelijke vermoedens, deskundigenonderzoek als bewijsmiddelen genoemd.[38] Ook de resultaten van onbemande cameracontrole worden door de rechtspraak aanvaard, maar de bewijswaarde daarvan wordt door de rechter vastgesteld.[39] Het watermerk zal in de praktijk dan ook zonder twijfel als wettig bewijsmiddel kunnen worden gekwalificeerd. Of het watermerk nog op andere gronden kan worden uitgesloten zal in de volgende paragrafen worden behandeld.

5.3 Watermerken als (on)rechtmatig verkregen bewijs

De toelaatbaarheid van het watermerk als bewijsmiddel wordt naast de kwalificatie als bewijsmiddel en de betrouwbaarheid ervan in de praktijk voor een belangrijk deel bepaald door het antwoord op vraag of het watermerk moet worden aangemerkt als een onrechtmatig verkregen bewijsmiddel en als gevolg daarvan van het bewijs moet worden uitgesloten. De vraag of het watermerk als bewijs moet worden uitgesloten kan bij watermerken in het geding komen wanneer er bij de inzet daarvan in strijd gehandeld is met het recht.[40] In de praktijk kan vooral worden gedacht aan de situatie waarin de rechthebbende in strijd heeft gehandeld met het recht op eerbiediging van de persoonlijke levenssfeer van de licentienemer (recht op privacy) door bij het verwerken van de persoonsgegevens in het watermerk in strijd te handelen met het recht.[41] De nadruk in deze paragraaf ligt op de schending van privacyrechten als grondslag voor het onrechtmatig handelen van de rechthebbende. Welke gevolgen aan verbonden moeten worden aan onrechtmatig verkregen bewijs wordt apart behandeld in paragraaf 5.4.

Om de rechtmatigheid van het watermerk als bewijsmiddel te beoordelen wordt eerst gekeken naar de vraag of watermerken mogelijk in strijd zijn met Europese grondrechten (par. 5.3.1). De bewijsbeoordeling en de mogelijke uitsluiting van bewijs vanwege schending van het recht laten het Europees Hof voor de Rechten van de Mens en het Hof van Justitie veelal over aan de nationale rechter en worden in het kader van mogelijk inbreuk op privacy dan ook

[37] Verstraeten 2012, 978; zie o.m. Cass. 10 april 1979, A.C. 1978-79, 953; Cass. 25 april 1996, A.C. 1996, 131; Cass. 2 maart 2011, RDPC 2011, 893.
[38] Verstraeten 2012, p. 980.
[39] Zie o.m. Cass. 21 januari 1992, A.R. 1992, 5332.
[40] Zie eerder uitgebreid de dissertaties van Embregts 2003 (diss.) en Kremer 1999 (diss.) en meer recent Asser 2013, p. 155.
[41] Het recht op eerbiediging van zijn persoonlijke levenssfeer is zowel verankerd in artikel 8 EVRM, artikel 7 Handvest EU, art 17 IVBPR, art. 12 UVRM als in de Nederlandse (art. 10) en de Belgische Grondwet (art. 22). De gegevens (naam en rekeningnummer) zoals deze verwerkt worden in het watermerk zijn persoonsgegevens op grond van artikel 2 onder a Richtlijn 95/46/EG zoals ook nationaal geimplementeerd in Nederland in artikel 1 onder a Wbp (par. 5.3.2.1) en in België in artikel 1, § 1 WVP (BE) (par. 5.3.2.2).

afzonderlijk besproken.[42] De vraag of en wanneer de rechthebbende inbreuk maakt op de privacyrechten van de licentienemer wordt naar nationaal recht besproken in paragraaf 5.3.2. Wanneer de rechter tot het oordeel zou komen dat de rechthebbende inbreuk heeft gemaakt op het recht van privacy van de licentienemer dan is in het strafrecht vooral de vraag of het Openbaar Ministerie (hierna: OM) bewijs mag gebruiken dat door de rechthebbende op een onrechtmatige wijze is verkregen (par. 5.3.3).

5.3.1 Grondrechten

Grondrechten kunnen een belangrijke rol spelen bij de toelaatbaarheid van watermerken als bewijs. In de Scarlet/Sabam-zaak toetste het HvJ EU een rechterlijk bevel waarin een internet service provider (ISP) werd verplicht een filter in te voeren ter handhaving van het auteursrecht onder het unierecht. Tegen de achtergrond van deze zaak kan ook het watermerk worden getoetst in een afweging tussen het auteursrecht en de andere grondrechten van de unie, waaronder het recht op privacy (par. 5.3.1.1). Over de rol van privacy bij de inzet van watermerken zijn al sinds de opkomst van watermerken in 2005 vragen gesteld, onder meer door Europese toezichthouders. Mede in dit licht ontwikkelde de Amerikaanse burgerrechtbeweging Center for Democracy & Technology (CDT) de 'Privacy Principles for Digital Watermarking' die veel overeenkomsten vertonen met huidige en toekomstige privacy-regelgeving in Europa. Ook deze meer technische beginselen bieden een goed uitgangspunt om de rechtmatigheid van watermerken te beoordelen (par. 5.3.1.2).

5.3.1.1 Watermerken in het licht van Europese grondrechten

In de discussie rondom de inzet van technologie bij de handhaving van het auteursrecht heeft het HvJ EU in de zaak Scarlet/Sabam de eerste kaders opgesteld naar aanleiding van de vraag of een Internet Service Provider (ISP) kan worden verplicht een filter in te voeren.[43] Het Hof van Beroep in Brussel had in deze zaak prejudiciële vragen aan het HvJ EU gesteld. In de kern ging deze zaak over de weigering van Scarlet om een systeem in te voeren waarbij elektronische communicatie via filesharingsoftware wordt gefilterd om daarmee met auteurs-rechten strijdige uitwisseling van bestanden te voorkomen.[44]

[42] Zie voor zaken waarin het EHRM de beoordeling van onrechtmatig bewijs in het licht van art. 6 EVRM (fair trail) over laat aan nationale gerechten o.m. EHRM 12 juli 1988, NJ 1988, 851 (Schenk); EHRM 12 mei 2000, NJCM Bulletin, p. 1255, m.nt. E. Myjer (Kahn/Verenigd Koninkrijk). In EHRM 9 juni 1998, NJ 2001, 471, m.nt. Kn (Texeira de Castro) kwam het Hof wel zelf tot een consequentie voor het onrechtmatig verkregen bewijs. Voor de verschillen met de eerdere uitspraken o.m. de annotatie onder dit laatste arrest. Het Hof beoordeelt de procedure in haar geheel en tegen het licht van het recht op een eerlijk proces (art. 6 EVRM). Het Hof komt in deze procedure tot het oordeel dat bewijs dat in strijd met privacyrechten (art 8 EVRM) is verkregen, niet noodzakelijk leidt tot oneerlijke procesvoering. Of daarvan sprake is moet mede beoordeeld worden tegen de achtergrond van het recht op tegenspraak, betrouwbaarheid van het bewijs en de vraag of de veroordeling heeft plaatsgevonden op meer dan één bewijsmiddel.

[43] HvJ EG 24 november 2011, zaak C-70/10, AMI 2011/2, m.nt. Dommering, Mf 2012/3, m.nt. Kulk & Borgesius (Scarlet/Sabam); zie ook HvJ EU 16 februari 2012, zaak C-360/10 (SABAM tegen Netlog), NJ 2012, nrs. 479 en 480, p. 5395-5397, m.nt. PBH (gezamenlijke noot voor beide arresten).

[44] Hof van Beroep 28 januari 2010, CR, 108, m.nt. B. Bruyndonckx (Sabam/Scarlet).

De Brusselse rechter wenst volgens het HvJ EU te vernemen of de uitleg van de richtlijnen inzake E-commerce- (2000/31), auteursrecht- (2001/29), handhaving- (2004/48), privacy- (95/46) en privacy en elektronische communicatie (2002/58), eraan in de weg staan dat een internetprovider door de rechter wordt gelast een filtersysteem in te voeren voor alle elektronische communicatie via zijn diensten. In deze zaak is komen vast te staan dat het systeem een preventieve werking heeft en op alle klanten van de ISP wordt toegepast. Tevens wordt het systeem uitsluitend door de ISP bekostigd en kent het in de tijd geen beperking. Het systeem zou verder in staat zijn om op het netwerk van deze provider het verkeer van elektronische bestanden die muzikaal, cinematografisch of audiovisueel werk bevatten, waarop de verzoeker intellectuele eigendomsrechten zou hebben, te identificeren en de overbrenging van bestanden waarvan de uitwisseling het auteursrecht schendt, te blokkeren (hierna: filtersysteem).[45]

Bij de beoordeling van die vraag stelt het Hof vast dat een dergelijk (algemeen) filtersysteem preventief toezicht vereist van alle elektronische communicatie op het netwerk van de betrokken internetprovider.[46] Een dergelijk bevel kan in strijd zijn met het algemene toezichtsverbod van artikel 15, lid 1 van de E-Commerce richtlijn (2000/31). Bij het beantwoorden van de vraag of een dergelijk bevel in overeenstemming is met het unierecht moet volgens het Hof ook rekening worden gehouden met de bescherming van toepasselijke grondrechten.[47]

Het Hof stelt vast dat het intellectuele eigendomsrecht een grondrecht vormt op grond van artikel 17, lid 2, van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest), maar dat het aan de autoriteiten en rechterlijke instanties is om voor de in dat kader vastgestelde maatregelen een juist evenwicht te verzekeren tussen de bescherming van deze rechten en de bescherming van de grondrechten van personen die door zulke maatregelen worden geraakt.[48]

---

[45] HvJ EG 24 november 2011, zaak C-70/10 (Scarlet/Sabam), ov. 29. Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, PB L 178, p. 1(E-commercerichtlijn); Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, PB L 167, p. 10 (Auteursrechtrichtlijn); Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PB L 157, p. 45, en rectificatie PB L 195, p. 16 (Handhavingsrichtlijn); Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281, p. 31), en Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (PB L 201, p. 37).

[46] De A-G en het Hof verschillen in de beantwoording op de prejudiciële vragen vanwege verschillende vertrekpunten. Zie ook uitgebreider Dommering 2012, p. 50.

[47] HvJ EG 24 november 2011, zaak C-70/10 (Scarlet/Sabam), ov. 38-41.

[48] HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), ov. 43-44 in navolging van HvJ EU 29 januari 2008, zaak C-275/06 (Promusicae), ov. 68. Later nogmaals herhaald in HvJ EU 19 april 2012, zaak C-461/10, (Bonnier Audio), ov. 56; HvJEU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien), ov. 47. Het Hof merkt tevens op (ov. 43) dat het intellectuele-eigendomsrecht weliswaar door artikel 17, lid 2, van het Handvest wordt beschermd, maar noch uit deze bepaling, noch uit de rechtspraak van het Hof vloeit voort dat dit recht

Vervolgens bespreekt het Hof drie grondrechten uit het Handvest: de vrijheid van ondernemerschap (art. 16), het recht op bescherming van persoonsgegevens (art. 8) en de vrijheid om informatie te ontvangen of te verstrekken (artikel 11).

Een bevel dat leidt tot de verplichting tot invoering van een permanent, duur en ingewikkeld informaticasysteem, is volgens het Hof niet alleen in strijd met artikel 3 lid 1, van de handhavingsrichtlijn, dat bepaalt dat de maatregelen ter bescherming van de intellectuele eigendomsrechten evenredig en niet onnodig ingewikkeld of kostbaar mogen zijn, maar vormt ook een ernstige beperking van de vrijheid van ondernemerschap.[49]

Het Hof houdt ook rekening met de effecten voor de klanten van de betrokken internetprovider vanwege mogelijke aantasting van de bescherming van persoonsgegevens en van hun vrijheid om informatie te ontvangen of te verstrekken. De aantasting van persoonsgegevens vindt het Hof in de systematische analyse van alle inhoud die het gebruik van het systeem veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen.[50]

Tot slot heeft het Hof aandacht voor de vrijheid van informatie die door het bevel kan worden beperkt, omdat niet duidelijk is of het systeem voldoende onderscheid maakt tussen legale en illegale inhoud en de toepassing zou kunnen leiden tot de blokkering van communicatie met legale inhoud.[51] Hierbij wijst het Hof erop dat het voor de beantwoording van de vraag of een verzending legaal is, ook afhankelijk is van de toepassing van wettelijke uitzonderingen op het auteursrecht. Daarbij kan niet alleen gewezen worden op de uitzonderingen die per lidstaat kunnen verschillen, maar ook op werken die in bepaalde lidstaten tot het publieke domein behoren of door de betrokken auteurs gratis op het internet zijn geplaatst.[52]

Het Hof komt tot de conclusie dat het juiste evenwicht ontbreekt tussen enerzijds het intellectuele eigendomsrecht en anderzijds, het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken. Een bevel tot het invoeren van het litigieuze filtersysteem is volgens het Hof dan ook in strijd met de bescherming van de toepasselijke grondrechten.[53]

---

onaantastbaar is en daarom absolute bescherming moet genieten. Het Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg heeft via art. 6 lid 1 Verdrag betreffende de Europese Unie (VEU of Unieverdrag) , 'dezelfde rechtskracht als de andere 'Verdragen'.

[49] Ov. 47-49; onder eerdere verwijzing van HvJ EU 12 juli 2011, zaak C-324/09(L'Oréal). Vgl. HvJ EU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien), ov. 48.

[50] HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), ov. 50-51. Zie voor IP-adressen als persoonsgegeven ook Wolters Ruckert 2012, p. 1.

[51] Vgl. HvJ EU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien) waarin het Hof oordeelt dat de genomen maatregelen de internetgebruikers niet nodeloos de mogelijkheid mogen ontzeggen om zich rechtmatig toegang tot de beschikbare informatie te verschaffen (ov. 56).

[52] HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), ov. 52.

[53] De Nederlandse en Belgische regering zijn algemeen van mening dat het recht van de Unie zich verzet tegen het vaststellen van een maatregel als de gevraagde. De Commissie is van mening dat de betreffende richtlijnen zich niet verzetten tegen het installeren van een filter- en blokkeringssysteem, maar dat de concrete vormen van het gebruik niet in overeenstemming zijn met het evenredigheidsbeginsel (AG Cruz Villalón d.d. 14 april 2011

Ondanks dat dit arrest ziet op een algemeen filtersysteem en niet kan worden uitgesloten dat andere systemen met andere specificaties de test van het Hof wel doorstaan, biedt dit arrest voorlopig een eerste toetsingskader voor de beoordeling van de vraag of watermerken in het licht van de Europese grondrechten toelaatbaar zijn.[54]

Het Hof stelt bij zijn beoordeling voorop dat de vastgestelde maatregelen een juist evenwicht moeten verzekeren tussen de bescherming van het intellectueel eigendomsrecht en de bescherming van de grondrechten van personen die door zulke maatregelen worden geraakt. Anders dan met het in dit arrest centraal gesteld filtersysteem wordt er bij watermerken van een derde noch een (algemene) toezichtsrol verwacht, noch zijn de kosten voor de invoering voor zijn rekening waardoor er in die zin geen reden is om aan te nemen dat iemand in zijn vrijheid van ondernemerschap wordt aangetast.

Voor watermerken is van groter belang dat er volgens het Hof een aantasting van persoonsgegevens plaatsvindt door de systematische analyse van alle inhoud die het gebruik van het systeem veronderstelt en kort gezegd de verzameling van persoonsgegevens van gebruikers die illegale inhoud via het netwerk versturen. Het Hof stelt vast dat IP-adressen de precieze identificatie van de gebruikers mogelijk maakt en derhalve persoonsgegevens vormen.[55] De beoordeling of hiervan sprake is hangt samen met de wijze waarop het werk wordt opgespoord en welke gegevens daarbij worden verzameld. Het opsporen van werken op het internet kan op vele manieren plaatsvinden. Om te voorkomen dat er in strijd gehandeld wordt met het recht op privacy zal er gekozen moeten worden voor een wijze waarbij in beginsel geen gegevens worden verzameld die de precieze identificatie van de gebruikers mogelijk maakt en derhalve persoonsgegevens vormen. Veel methoden sporen overigens enkel de werken op en verzamelen geen persoonsgegevens anders dan gegevens die in de werken zijn aangebracht, zoals in de metadata. Anders dan bij het filtersysteem in deze zaak leidt een ‘hit’ bij watermerken niet onmiddellijk en automatisch tot het uitsluiten van deze content voor alle gebruikers. Watermerken met een traitortracingsdoel hebben enkel tot doel de licentienemer op te sporen. Van het uitsluiten van content voor gebruikers is in technisch opzicht geen sprake. De content blijft voor iedereen te gebruiken. Naast het uitsluiten speelt in de overweging van het Hof mee dat een ‘hit’ veelal onmiddellijk en automatisch tot een sanctie leidt. Hieruit maak ik op dat het Hof een systeem dat veelal onmiddellijk en automatisch een sanctie uitdeelt mogelijk in strijd acht met subsidiariteitsbeginsel. Het is niet ondenkbaar dat het Hof hierbij laat mee spelen dat in dit geval ook de sanctie (uitsluiten) behoorlijk zwaar is, terwijl een gebruiker niet kan opkomen tegen een systeem dat veelal onmiddellijk en automatisch tot een sanctie overgaat. Anders dan het hier bedoelde filtersysteem heeft watermerken met een traceerdoel niet als doel om direct een (technische) sanctie op te leggen. In het kader van het beschermen van privacy is het niet ondenkbaar dat

inzake Scarlet/Sabam, ov. 35). Zie ook Jaarbericht 2011. Procesvertegenwoordiging Hof van Justitie van de EU. De inbreng van de Nederlandse regering, bijlage bij Kamerstukken II 2011-2012, 33000-V nr. 143.

[54] Zie een bespreking en vergelijkbare conclusies ook Dommering 2012, p. 50.; Chavannes 2013, p. 196.

[55] HvJ EU 24 november 2011, zaak C-70/10, ov. 51.

het Hof ook terughoudend is bij het detecteren en uitlezen van persoonsgegevens bij watermerken.[56] Bij watermerken begint het uitlezen van de gegevens van de licentienemer pas bij het aantreffen van gelijkend werk. Wanneer dit werk is aangetroffen zal men moeten vaststellen of er sprake is van inbreuk op het auteursrecht. Zoals eerder besproken speelt het watermerk bij die vaststelling in beginsel geen rol.[57] Pas nadat de rechthebbende heeft geconstateerd dat er sprake is van een inbreuk op het auteursrecht komt hij in beginsel toe aan het detecteren en uitlezen van het watermerk. Het vaststellen dat er sprake is van inbreuk op het auteursrecht kan zowel automatisch als handmatig plaatsvinden.[58] Door nogmaals (handmatig) de inbreuk te beoordelen kan worden voorkomen dat de licentienemer ten onrechte wordt aangesproken op inbreuk op het auteursrecht, bijvoorbeeld omdat er sprake is van een wettelijke uitzondering. Daarmee zou tegelijk tegemoet worden gekomen aan het Hof dat in het kader van de vrijheid van informatie duidelijk maakte dat het onwenselijk is dat er onvoldoende onderscheid gemaakt wordt tussen legale en illegale inhoud.[59] Het Hof koppelt dit onderscheid in dit arrest overigens aan de toepassing die ertoe zou kunnen leiden dat communicatie met legale inhoud wordt geblokkeerd. Van dit laatste is bij watermerken, zoals eerder gezegd, geen sprake. Wanneer een watermerk wordt gedetecteerd en succesvol kan worden geïnterpreteerd zal de sanctie beperkt zijn tot het aanspreken van de licentienemer. De impact van het systeem is in die zin beperkt tot de licentienemer en beperkt de vrijheid van informatie van anderen in beginsel niet.[60] Niettemin zou men er in het licht van dit arrest verstandig aan doen om naast een softwarematige controle op inbreuk ook een controle-mechanisme in te bouwen ten aanzien van de wettelijke uitzonderingen. Om te voorkomen dat er in strijd gehandeld wordt het recht op privacy zal er tevens gekozen moeten worden voor een opsporingsmethode waarbij in beginsel geen gegevens worden verzameld die de precieze identificatie van de gebruikers mogelijk maakt en derhalve persoonsgegevens vormen.

Behoudens een mogelijke inbreuk op privacyrechten van de licentienemer is er vooralsnog weinig reden om aan te nemen dat het Hof van Justitie EU afwijzend zou staan tegenover het gebruik van watermerken. Over mogelijke inbreuk op privacy wordt ingegaan in de volgende (sub-)paragraaf.

---

[56] Vgl. EHRM 5 oktober 2010, NJB 2011, 236, NJ 2011/566 m.nt. EJD (Köpke/Duitsland) waarin het EHRM slechts inbreuk op privacy toestond na een afweging van belangen en de constatering dat de inbreuk tot zo beperkt mogelijk is gebleven. Zie verder par. 5.3.2.

[57] Zie hoofdstuk 3 auteursrecht, par. 3.4. Het watermerk kan wel informatie bevatten over de afgesloten licentie en aangeven of de rechthebbende gerechtigd is om het werk bijvoorbeeld op internet te zetten. In de regel is de licentienemer hiertoe echter niet gerechtigd, zodat de vraag in de praktijk nauwelijks een rol speelt.

[58] Strikt genomen kan alleen de rechter inbreuk op het auteursrecht vaststellen. Waar het om gaat is dat de rechthebbende vast stelt dat er naar zijn mening sprake is van inbreuk op het auteursrecht (par. 3.4).

[59] Ov. 52, waarin het Hof ook opmerkt dat ‘de beantwoording van de vraag of een verzending legaal is, ook afhangt van de toepassing van wettelijke uitzonderingen op het auteursrecht, die verschillen van lidstaat tot lidstaat’. Vgl. HvJ EU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien) waarin het Hof oordeelt dat de genomen maatregelen de internetgebruikers niet nodeloos de mogelijkheid mogen ontzeggen om zich rechtmatig toegang tot de beschikbare informatie te verschaffen (ov. 56).

[60] Hierbij moet worden opgemerkt dat de vrijheid van informatie altijd wordt geraakt wanneer men informatie van het internet afhaalt. Vgl. Dommering 2012, p. 50. ‘De vrijheid van informatie floreert bij het kennisnemen van clandestiene informatie’.

5.3.1.2 Aandacht voor privacy bij de opkomst van watermerken

Met de opkomst van watermerken en de toepassingsmogelijkheden daarvan is er ook aandacht gekomen voor privacyaspecten van watermerken. In 2005 uitte de Europese Data Protection Working Party in haar werkdocument over gegevensbescherming in relatie tot intellectuele eigendomsrechten vooral de zorg dat gebruikers zich moeten identificeren voordat zij content officieel kunnen downloaden en dat hun profiel verder gecomplementeerd kan worden doordat unieke codes in ieder stuk gedownloade content worden aangebracht.[61] De werkgroep heeft er met name bezwaar tegen dat elke gebruiker en ieder aangekocht werk kan worden gevolgd. Zij pleiten er dan ook voor dat de content niet gelinkt wordt aan een individu tenzij dit nodig is voor de uitvoering van de service dan wel wanneer de gebruiker geïnformeerd is en hierin heeft toegestemd. In reactie daarop heeft de Digital Watermarking Working Group (DWWG), die bestond uit de elf (leidende) watermerkleveranciers, een antwoord geformuleerd dat er in de kern op neer komt dat digitale watermerken content helpen identificeren en niet de individuele gebruiker. Zij stellen: 'In most if not all commercial applications, digital watermarks carry data that is not linked to an individual in any way, but rather, behaves as an essential and effective content identifier'.[62] Deze stelling is in het licht van de bekende zaak Warner Bros/Caridi uit 2004 op zijn minst opmerkelijk, omdat de geopenbaarde films uiteindelijk met behulp van watermerken aan de acteur Caridi konden worden gekoppeld.[63] De opmerkingen van de werkgroep waren wellicht soms te generalistisch, maar de reactie daarop vanuit de industrie deed ook niet volledig recht aan de zorgen vanuit de werkgroep.

In mei 2008 kwam Amerikaanse burgerrechtbeweging Center for Democracy & Technology (CDT), met 'Privacy Principles for Digital Watermarking'.[64] Zij vangen deze privacy-beginselen aan met de constatering dat watermerktechnologie een algemene toepassing is met veel gebruiksmogelijkheden en zonder inherente privacyrisico's. In dat kader wijzen zij erop dat watermerken al enige tijd worden ingezet en zij niet bekend zijn met problemen rondom privacy of misbruik.[65] Hoewel zij ook andere toepassingen behandelen concentreren zij zich vooral op watermerken met een traceerdoel.[66] Het CDT heeft acht beginselen geformuleerd: (1) Privacy by design, waarmee wordt bedoeld dat er vanaf het begin van de ontwikkeling aandacht moet zijn voor privacy; (2) Vermijd direct bruikbare informatie, zodat zelfs wanneer

[61] Working document on data protection issues related to intellectual property rights
January 18, 2005, Article 29 Data Protection Working Party, p. 3, 5.
[62] Digital Watermarking Working Group's Response to Privacy Concerns Raised by Paper WP 104 from the European Union's Data Protection Working Party, 31 Mar 2005, p. 4.
[63] United States District Court, Central District of California, 18 november 2004, 346 F. Supp. 2d 1068 (Warner Bros/Carmine Caridi et al.).
[64] Deze beweging is in Nederland waarschijnlijk het beste te vergelijken met Bits of Freedom (BOF). Zij presenteerde in 2008 haar Privacy Principles for Digital Watermarking, May 2008 – Version 1.0. (pagina's zijn ongenummerd) https://www.cdt.org/copyright/20080529watermarking.pdf.
[65] Privacy Principles for Digital Watermarking, May 2008 – Version 1.0, eerste pagina. Ook in de periode daarna (tot december 2013) heb ik geen problemen rondom privacy of misbruik waar genomen.
[66] p. 5 'Watermarks embedded in infringing copies of copyrightedmedia content could enable copyright holders to trace the copies back to particular users or distributors, and potentially to launch legal action.'

de informatie openbaar wordt deze niet direct bruikbaar is; (3) Informeer de gebruiker; (4) Beperk de toegang tot het uitlezen van watermerken, zodat het uitlezen van deze watermerken niet eenvoudig is; (5) Reageer adequaat als de watermerkalgoritmen zijn gekraakt; (6) Bescherming van de databanken; (7) Beperk het gebruik voor andere doeleinden en tot slot (8) de zorg voor toegang en wijzigingsmogelijkheden voor gebruikers. Deze beginselen zijn thans ook opgenomen in de verschillende privacyrichtlijnen en nationale wetgeving zoals privacy by design, het gebruik van algemene nummers in plaats van persoonsgegevens, het informeren van de gebruiker en het nemen van voldoende technische en organisatorische maatregelen.[67] Ook komen zij waarschijnlijk terug in de nieuwe Europese privacyverordening waarin opnieuw kaders worden gegeven voor een zorgvuldige omgang met persoonsgegevens.[68]

Deze beginselen leveren dan ook een concreet toetsingskader op voor het toetsen van watermerken aan Europese privacyrichtlijnen en de implementatie daarvan in de Nederlandse en Belgische wetgeving. Een nadere invulling wordt op grond van Europese privacy-richtlijnen nog aan de nationale wetgever, de toezichthouder en rechtspraak overgelaten maar wordt na de toepasselijkheid van de nieuwe privacyverordening de verantwoordelijkheid van de Europese toezichthouders en de Europese rechtspraak.[69] Voor watermerken in dit onderzoek kunnen de 'Privacy Principles for Digital Watermarking' dan ook een concreet toetsingskader vormen.

(1) Privacy by design

Het eerste beginsel ziet op Privacy by design, waarmee wordt bedoeld dat er vanaf het begin van de ontwikkeling aandacht moet zijn voor privacy. Dat deze aandacht er is en op welke wijze hier aan kan worden bijgedragen zal worden behandeld in de hierna volgende beginselen.

(2) Vermijd direct bruikbare informatie

Het tweede beginsel ziet op het vermijden van direct bruikbare informatie, zodat zelfs wanneer de informatie openbaar wordt deze niet direct bruikbaar is. Zoals reeds besproken in

[67] In Nederland heeft het CBP in februari 2013 een richtsnoeren uitgegeven voor de beveiliging van persoonsgegevens. Hiermee geeft het CBP nader invulling aan wat passende technische en organisatorische maatregelen kunnen inhouden reken houdend met de stand van de techniek.
http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[68] Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), Brussel, 25 januari 2012, COM(2012)11 def., 2012/0011 (COD). Zie voor een nadere uitwerking van de wijze waarop de rechthebbende dat naar huidig Nederlands recht moet doen, o.m. Thole e.a. 2010.

[69] De belangenorganisatie van webwinkels Thuiswinkel.org maakt 27 februari 2013 op haar website bekend dat zij van mening is dat het CBP samen met zijn Europese zusterorganisaties te veel 'ondemocratische' invloed heeft op ten aanzien van de invulling van (Europese) privacywetgeving.
http://www.thuiswinkel.org/persberichten/toezichthouders-kapen-europees-privacybeleid

hoofdstuk 2 bevat het watermerk een reeks cijfers en/of letters (code) die verwijst naar de licentienemer. De gegevens van de licentienemer kunnen op twee verschillende niveaus worden beschermd. Ten eerste is er sprake van technische bescherming doordat de code niet direct toegankelijk is voor gebruikers van de gewatermerkte content doordat watermerken-technieken deze code zowel verbergen (steganografie) als versleutelen (cryptografie).[70] Ten tweede kan er sprake zijn een organisatorische bescherming doordat de code, zonder tussenkomst van een derde, voor rechthebbende niet-direct herleidbaar is tot de persoons-gegevens van de licentienemer. Dit kan op verschillende manieren worden bewerkstelligd. Ten eerste kan de rechthebbende het organisatorisch zo inrichten dat degene die zich bezig houden met handhaving niet direct toegang hebben tot de databank waarmee de code in het watermerk en de persoonsgegevens van de licentienemer gekoppeld kunnen worden. Ten tweede kan worden gedacht aan een onafhankelijke derde, zoals een Trusted Third Party (TTP) die na het vaststellen van de inbreuk door de rechthebbende de koppeling legt tussen de code en de licentienemer en deze laatste gegevens verstrekt. In beide gevallen is het wenselijk dat er een afweging plaatsvindt voor het verstrekken van deze persoonsgegevens. Hiervoor zou aansluiting kunnen worden gezocht bij de criteria van Lycos/Pessers waarin uiteindelijk de Nederlandse Hoge Raad tot zorgvuldigheidscriteria komt die het mogelijk maken om de NAW-gegevens aan een derde te verstrekken.[71] Met deze maatregelen wordt de toegang tot het uitlezen van watermerken beperkt. Vanzelfsprekend zal daarbij nader invulling gegeven moeten worden aan de kring van bevoegde personen en daarmee samenhangende criteria.

Of hiermee ook wordt voldaan aan het tweede beginsel is ook afhankelijk van de vraag of de versleutelde code (watermerk) al dan niet tot identificeerbaarheid van de persoon leidt dan wel voldoende anonimiseert. Anders gezegd is het de vraag of de versleutelde code (watermerk) nog wel een persoonsgegeven is. Wanneer deze code geen persoonsgegeven, maar een procesgegeven is, dan is de privacyregelgeving verder niet van toepassing.
Of een persoon te identificeren is, vormt dus een belangrijk element voor de vraag of sprake is van een persoonsgegeven.[72] Op grond van de richtlijn geldt ook naar Nederlands en Belgisch recht als uitgangspunt dat een persoon identificeerbaar is, indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. In dat kader spreekt men van indirect identificeerbare gegevens wanneer deze gegevens niet direct tot identificatie van een bepaald persoon leiden, maar via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.[73]

[70] Zie par. 2.2.3.
[71] Zie par. 5.3.2.1.
[72] Artikel 1 onder a Wbp. Artikel 1, §1 WVP (Belgische Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992, B.S., 18 maart 1993). In Nederland blijkt uit de kamerstukken dat uit de aard van de gegevens of de context waarin de gegevens worden vastgelegd en gebruikt, alsmede het gebruik van de gegevens kan blijken dat het een persoonsgegeven betreft. Hierbij moet worden gedacht aan de wijze waarop een persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Kst II 1997/1998, 25892, nr. 3, p. 46.
[73] Zie in Nederland Kst II 1997/1998, 25982, nr. 3, p. 47-48; in België Kamer 1997-98, 1566/1, p. 12. Zie in dat kader ook ov. 27 van de Richtlijn (95/46/EG). Zie o.m. CPBL, Beraadslaging NR 04/031 van 7 september 2004 m.b.t. de medeling van gecodeerde sociale gegevens van persoonlijke aard en anonieme gegevens aan de

Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enige andere persoon in te zetten zijn om genoemde persoon te identificeren.[74] Daarbij is onder meer relevant of er doeltreffende maatregelen zijn getroffen die identificatie redelijkerwijs uitsluiten (privacy by design of Chinese Walls).[75] Ook daarbij geldt dat wanneer identificatie met behulp van andere bestanden mogelijk is, de code nog steeds als een persoonsgegeven geldt.[76] Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten, en dergelijke van de verantwoordelijke.[77]

Om te voorkomen dat de rechthebbende kennis heeft van het watermerk en daarmee het watermerk ook achteraf kan plaatsen zijn er in de watermerkliteratuur voorstellen gedaan om een Trusted Third Party (TTP) te gebruiken om dit probleem te voorkomen. Eenzelfde oplossing is denkbaar voor het beschermen van privacy van licentienemers. De inzet van een TTP die de NAW-gegevens gescheiden houdt, betekent echter nog niet dat er geen sprake (meer) is van persoonsgegevens. Deze gegevens kunnen, ook als deze geen NAW-gegevens bevatten, als indirect identificerende gegevens worden aangemerkt wanneer zij via nadere stappen met een bepaald persoon in verband kunnen worden gebracht.[78] De Wbp blijft enkel buiten toepassing wanneer er geen persoonsgegevens worden verwerkt. Daarvan is enkel sprake wanneer de code is ontdaan van alle (in)directe identificerende kenmerken die het mogelijk maken om die gegevens te herleiden tot de licentienemer en deze (in)direct identificerende gegevens ook niet meer tot identificatie kunnen leiden. Dit betekent in ieder geval naar Nederlands recht dat het achteraf ook niet met andere technieken mogelijk moet zijn de gegevens te koppelen waardoor de licentienemer alsnog kan worden geïdentificeerd.[79]

Dat betekent dat identificatie redelijkerwijs moet zijn uitgesloten. Hoe lastig dat is wordt duidelijk in de zaak van de Nederlandse Spoorwegen (NS) over de OV-studentenkaart. In deze zaak wordt duidelijk dat het onvoldoende is wanneer men overgaat tot het (1) anonimiseren van klantgegevens tot het niveau van BSN (geen NAW-gegevens), (2) deze vervolgens converteren naar een 'OV-ID' en (3) op basis hiervan de gegevens naar een derde versturen, die de studentenkaart klaar zet (4) waardoor de NS als vervoerder uitsluitend

federale overheidsdienst met het oog op het uitbouwen van een microsimulatiemodel voor de sociale zekerheid en een sociale zekerheidsmatrix, ov. 5.

[74] Kst II 1997/1998, 25982, nr. 3, p. 48.

[75] Privacy by Design ziet op het fenomeen dat ontwikkelaars ontwerpen daarvan na te denken over waarborgen om persoonsgegevens te beschermen en te beveiligen. Zie Borking 2010, p. 389; CBP reactie op plan Eurocommissaris Reding voor herziening privacyrichtlijn reactie: Privacy by design onontbeerlijk in ICT-tijdperk. Mededeling, 4 november 2010. Chinese Walls refereren aan 'muren' die een scheiding aanbrengen tussen bijvoorbeeld afdelingen of systemen waardoor ze niet met elkaar in aanraking kunnen komen.

[76] Kst II 1997/1998, 25982, nr. 3, p. 49 en advies 4/2007, p. 18.

[77] Kst II 1997/1998, 25982, nr. 3, p. 48-49, Richtlijn 95/46/EG, ov. 26.

[78] Kst II 1997/1998, 25982, nr. 3, p. 48. Zie voor de omstandigheden waaronder een nummer een persoon kan identificeren ook Werkgroep artikel 29; zie over het begrip persoonsgegeven advies 4/2007, p. 13

[79] Koorn e.a. 2004, p. 39 (PET witboek voor beslissers).

'anonieme reizigers' ziet bij een kaartcontrole.[80] De hierboven beschreven en door de NS toegepaste stappen vormen volgens het College Bescherming Persoonsgegevens (hierna: Cbp) niet de benodigde Privacy by Design en de technische en organisatorische Chinese Walls (art. 13 WBP) en leiden niet tot de conclusie dat identificatie redelijkerwijs is uitgesloten. Onduidelijk is wanneer identificatie redelijkerwijs wel is uitgesloten.[81] Dat betekent voor de inrichting van het watermerksysteem dat er niet snel voldaan zal zijn aan het tweede beginsel van het vermijden van direct bruikbare informatie. In de regel zal de versleutelde code al snel een persoonsgegeven in de zin van het privacyrecht (de Wbp) bevatten.[82] Dat heeft tot gevolg dat rechthebbenden moeten voldoen aan Europese en nationale zorgvuldigheidsnormen in het kader van privacyrecht en dat schending daarvan onrechtmatig is en uiteindelijk kan leiden tot de vaststelling dat aldus verkregen bewijs onrechtmatig verkregen is.

(3) Informeer de gebruiker

Als derde beginsel geldt dat de gebruiker geïnformeerd moet worden. De rechthebbende is bij gebruik van de persoonsgegevens van de licentienemer verplicht hem in te lichten over het verwerken van zijn gegevens alsmede over het doel van de verwerking.[83] Dit geldt te meer omdat de licentienemer door het verborgen karakter van het watermerk zich niet eenvoudig op de hoogte kan stellen van het verwerken van zijn persoonsgegevens. Ten aanzien van de heimelijkheid geldt in het algemeen dat het feit zelf nog geen inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer oplevert, maar dat daarvoor bijkomende omstandigheden vereist zijn.[84] Bij het informeren van de gebruiker is het ook van belang of hij bepaalde verwachtingen mag hebben over de inzet van auteursrechtelijke handhavingsinstrumenten.[85] In 2006 oordeelde het Hof Amsterdam nog dat iemand die zijn computer openstelt voor p2p er niet op bedacht hoeft te zijn dat een organisatie zijn 'shared

[80] Cbp 9 juni 2011, z2011/00057 (CBP/NS). Zie voor een beschrijving van deze casus ook Katus 2012. Het chipnummer in deze zaak bv. 'MediaID: 261864339' is gescheiden van het kaartnummer bv. 6789012345, waardoor persoonsgegevens op de kaart gescheiden blijven van het chipnummer.

[81] Zie Katus 2012, p. 45 die op persoonlijke titel, maar destijds werkzaam als Privacy Officer bij de NS, tot de conclusie komt dat de stijl van handhaven feitelijk neer komt op een disincentive voor organisaties om nog in privacy by design te investeren omdat anonimiseringsmaatregelen de toezichthouder kennelijk nooit ver genoeg gaan.

[82] Of dezelfde conclusie kan worden getrokken naar Belgisch recht hangt af van de beoordeling daarvan in België die tot nu toe nog niet in een zaak naar voren is gekomen.

[83] EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, NJB 2011, 236, NJ 2011/566 m.nt. EJD (Köpke/ Duitsland); EHRM 3 april 2007, R.D.T.I. 2007, (371) 371, m.nt. NJ 2007-50, nr. 617, p. 6232-6236, m.nt. EJD (Copland/Verenigd Koninkrijk). De kantonrechter (Haarlem 24 mei 2006, JAR 2006/197) achtte het het voldoende dat de werknemer via de ondertekende kassiersovereenkomst op de hoogte was gesteld, van steekproefsgewijze controle tijdens de kassadienst en het voorbehoud van de werkgever ten aanzien van het gebruik van verborgen camera's.

[84] Zie voor heimelijke video-opname o.m. Hof 's-Hertogenbosch 2 juli 1986, ECLI:NL:GHSHE:1986:AC9463 (Koma) o.v. 4.2. Zie voor heimelijk opgenomen telefoongespreken: HR 16 oktober 1987, ECLI:NL:HR:1987: AC9997, NJ 1988, 850, m.nt EAA (Dreissen/Van Gelder), ov. 3.3.3; HR 7 februari 1992, NJ 1993, 78 m.nt. HJS, VN 1992, 1564, m. nt. Red. (Slempkes/Nool), ov. 3.5.3.; Rb. Amsterdam 30 augustus 2010, ECLI:NL:RBAMS: 2010:BP1423, ov. 9. In beide gevallen kwam de rechter overigens niet toe aan de uitsluiting van het bewijs omdat zij geen inbreuk geconstateerde op de persoonlijke levenssfeer.

[85] Zie over deze verwachtingen o.m. de noot van Dommering onder de zaak Copland/Verenigd Koninkrijk (EHRM 3 april 2007, NJ 2007-50, nr. 617, p. 6232-6236) over het voeren van telefoongesprekken in callcentra.

folder' bekijkt op mogelijke inbreuken op auteursrecht.[86] De bekendheid van dit arrest, maar ook de ontwikkelingen en aandacht voor cookies, spam en virussen leiden tot de vraag of internetgebruikers hier tegenwoordig niet op bedacht moeten zijn. Daarnaast zou ook gesteld kunnen worden dat het een feit van algemene bekendheid is dat erop internet veel inbreuk op het auteursrecht plaatsvindt en dat het internet ook door rechthebbenden wordt gemonitord.[87] Hiermee is echter niet gezegd dat de gebruiker niet geïnformeerd hoeft te worden, maar slechts dat de heimelijkheid van het watermerk op zichzelf in beginsel onvoldoende grond oplevert voor het schenden van de persoonlijke levenssfeer.

De inlichtingenplicht is gebaseerd op privacywetgeving.[88] Verder valt te denken aan nieuwe wetgeving waarin onder andere bij cookies ook op Europees niveau geïnformeerde toestemming van de internetgebruiker is vereist.[89] Door het niet naleven van deze inlichtingenplicht handelt de rechthebbende in beginsel onrechtmatig tegenover zowel handelaren als niet-handelaren (consumenten). In de regel zal zowel de toestemming als de informatie door de rechthebbende weinig problemen opleveren. De licentienemer zal wanneer hij toegang wil hebben tot de werken zich genoodzaakt zien zijn toestemming te geven voor het verwerken van zijn persoonsgegevens. Wanneer hij geen toestemming verleent zal hij geen toegang krijgen tot werken.[90] De rechthebbende zal zijn licentienemer niet alleen willen informeren vanuit het oogpunt van privacyrecht, maar vooral vanuit de gedachte dat de preventie werking van watermerken gebaat is bij een goede informatie over de aanwezigheid van watermerken. In relatie tot privacy kan hij de licentienemer er ook op wijzen dat, hoewel zijn gegevens versleuteld zijn, hij ook zelf zijn privacy het beste kan beschermen door het werk niet te verspreiden. De rechthebbende kan ook met toestemming en na informatie van de licentienemer onrechtmatig handelen door in strijd met de richtlijn en de geïmplementeerde nationale wetgeving te handelen of door aanwijzingen van de nationale toezichthouder niet op te volgen.[91] In de praktijk vormt de toestemming of kenbaarheid van watermerken nauwelijks een probleem, omdat nagenoeg alle gebruikersbepalingen hier aandacht voor hebben.[92] Zo meldt bijvoorbeeld Bol.com direct bij de beschrijving van het boek dat het e-boek een watermerk bevat.[93]

---

[86] Hof Amsterdam 13 juli 2006, ECLI:NL:GHAMS:2006:AY3854, CR 2006, 168 m. nt. N.M. Wisman (Brein/Kazaa).
[87] Ten aanzien van de algemene bekendheid kan worden verwezen naar o.m. De Cock Buning & Van Eek 2009, p. 224 en Hugenholtz 2008, p. 581.
[88] Zie o.m. Hof 's-Hertogenbosch 2 juli 1986, ECLI:NL:GHSHE:1986:AC9463, NJ 1987, 451 (Koma).
[89] Zie voor het gebruik van cookies (plaatsen en uitlezen) o.m. Borgesius 2011, p. 2. Vgl. ook de minister die bij de Nota bij het verslag bij Wijziging van de artikelen 139f en 441b van het WvSr (uitbreiding strafbaarstelling heimelijk cameratoezicht) opmerkte dat 'heimelijk gebruik van camera's ter opsporing van strafbare feiten (bijv. diefstal of fraude) is in beginsel is voorbehouden aan de politie'. Daarbij neemt de minister kennelijk aan dat de burger in dat kader ook een beroep kan doen op de politie (vgl. cameratoezicht). Kst II 2000/01, 27 732, nr. 5, p. 14. De vraag is echter of de burger daar in de praktijk ook terecht kan.
[90] Zie ook Alberdink Thijm 2001, p. 73.
[91] Zo kan er in strijd gehandeld worden met het inzage- en correctierecht, maar kan de rechthebbende ook onvoldoende technische en organisatorische maatregelen hebben genomen om te kunnen spreken van een zorgvuldige verwerking van persoonsgegevens.
[92] Zie specifiek voor watermerken, o.m. de algemene voorwaarden bij de e-boeken van Harry Potter.
[93] Zie bijvoorbeeld http://www.bol.com/nl/p/wachten-op-woensdag/9200000014099364/

(4) Beperk de toegang tot het uitlezen van watermerken

Het vierde beginsel ziet op het beperken van de toegang tot het uitlezen van watermerken en betreft een bij beginsel drie reeds besproken technische en organisatorische maatregel. Of dat voldoende is zal mede in het licht van de stand van de techniek moeten worden bepaald alsmede naar de stand van de wetenschap in het kader van informatiebeveiliging.[94]

(5) Reageer adequaat als de watermerkalgoritmen zijn gekraakt

Het vijfde beginsel houdt in dat de rechthebbende adequaat moet reageren als de watermerkalgoritmen zijn gekraakt. Hiermee wil men vooral uitdrukking geven aan het feit dat er duidelijkheid moet komen voor alle betrokken over de voorgevallen kraak. Dit beginsel is in haar doelstelling vergelijkbaar met de in Europees en nationaal verband voorgestelde waarschuwingen bij datalekken.[95]

(6) Bescherming van de databanken
De bescherming van de databanken dat als zesde beginsel is opgenomen is vergelijkbaar met de huidige bepaling rondom technische en organisatorische maatregelen.[96]

(7) Beperk het gebruik voor andere doeleinden

Het zevende beginsel ziet op de beperkingen rondom het gebruik voor andere doeleinden. Hierbij wordt expliciet verwezen naar 'mission creep'. Het is voorlopig lastig om te bepalen voor welke doeleinden deze gegevens nog meer gebruikt zouden kunnen worden. Voor de in dit onderzoek bedoelde watermerken geldt dat observatie van gedrag van consumenten mede gegeven de context waarin het watermerk wordt gebruikt vooralsnog niet mogelijk is waardoor inbreuk op privacyrecht in dat opzicht geen rol speelt.

(8) Zorg voor toegang en wijzigingsmogelijkheden voor gebruikers

Tot slot ziet het achtste beginsel op de zorg voor toegang en wijzigingsmogelijkheden voor gebruikers, zoals deze thans ook is opgenomen in de privacyrichtlijnen en nationale wetgeving.[97]
Het is onduidelijk of en zo ja welke van deze beginselen in de praktijk worden nageleefd en op welke wijze daaraan invulling wordt gegeven. Rechthebbenden doen er verstandig aan om

[94] Zie daarvoor naar Nederlands recht ook het eerder genoemde richtsnoer van het CBP (2013).
[95] Zie o.m. de Europese Privacy Verordening en het Nederlandse wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens (gebruik camerabeelden en meldplicht datalekken).
[96] Richtlijn 95/46/EG, art. 4 van 2002/58/EG; art. 13 Wbp (NL), art. 16 WVP (BE).
[97] Het gaat hier om recht op kennisneming, verbeteren, aanvullen, verwijderen, afschermen, van verzet en het recht om gevrijwaard te blijven van geautomatiseerde individuele besluitvorming. Zie o.m. art. 36 Wbp (NL); art. 9 WVP (BE).

bij het afnemen van een watermerkservice aandacht te hebben voor deze richtlijnen. Van professionele aanbieders mag worden verwacht dat zij handelen op basis van deze richtlijnen, mede omdat zij niet onbekend zijn met privacyvraagstukken rondom watermerken, getuige hun eerder besproken reactie op het werkdocument van de Europese Data Protection Working Party.[98] Ten tweede zijn zij, vanwege hun klanten, gebaat bij het naleven van de eerder genoemde beginselen. Het naleven van deze richtlijnen zal immers bijdragen aan de acceptatie van het watermerk, zowel door consumenten als door rechters die uiteindelijk een oordeel moeten geven wanneer een watermerk als een juridisch bewijsmiddel wordt gepresenteerd. Tot op heden zijn mij geen incidenten of stelselmatige inbreuken bekend op de privacyrechten van licentienemers. Ook het CDT wijst erop dat ondanks de inzet van watermerken zij niet bekend zijn met problemen rondom privacy of misbruik.[99] Niettemin zou inbreuk op privacyrechten in Nederland en België voor het watermerk kunnen leiden tot de kwalificatie van onrechtmatig verkregen bewijs. De gevolgen daarvan worden apart besproken in paragaaf 5.4. Naarmate watermerken concretere informatie kunnen verschaffen over gedragingen van individuen en naarmate het belang van privacy maatschappelijk toeneemt, zal een privacytoets bij watermerken aan belang winnen.

5.3.2 Civielrechtelijke onrechtmatigheid

In de voorgaande paragraaf is duidelijk geworden dat het in strijd handelen met de privacyrechten van de licentienemer de voornaamste grondslag zal vormen ten aanzien van de vraag of het watermerk als bewijsmiddel als een onrechtmatig verkregen bewijsmiddel gekwalificeerd kan worden.[100] In de twee navolgende paragrafen wordt op basis van het Nederlandse en Belgische nationale recht nader onderzocht onder welke voorwaarden de rechthebbende de persoonsgegevens van de licentienemer mag verwerken in het watermerk. Wanneer de rechthebbende op onjuiste wijze is omgegaan met de persoonsgegevens van de licentienemer kan er sprake zijn van onrechtmatig handelen ten aanzien van de licentienemer.[101]

Zowel de Nederlandse als de Belgische wet inzake de bescherming van persoonsgegevens komen voor een belangrijk deel voort uit de Europese privacyrichtlijn en hebben om die reden vergelijkbare bepalingen ten aanzien van de voorwaarden waaronder de gegevens in het watermerk mogen worden verwerkt. Omdat het Nederlandse recht leidend is in dit onderzoek

[98] Digital Watermarking Working Group's Response to Privacy Concerns Raised by Paper WP 104 from the European Union's Data Protection Working Party, 31 Mar 2005, p. 4.

[99] Privacy Principles for Digital Watermarking, May 2008 – Version 1.0, eerste pagina.

[100] Naast het algemene onrechtmatige daadsrecht (zorgvuldigheidsnormen) en het privacyrecht kunnen voor watermerken ook regels van consumentenrecht en contractenrecht gelden, maar deze worden verder buiten beschouwing gelaten. Zie voor de hoofdlijnen daarvan par. 4.3.

[101] Met behulp van de in dit onderzoek bedoelde watermerken is het momenteel niet mogelijk gedrag van consumenten op internet te observeren. Daar komt bij dat het systeem in die zin in beginsel ook tegen de licentienemer werkt, omdat hij enkel 'gevonden en geobserveerd' kan worden wanneer hij zelf op een onrechtmatige wijze het werk openbaar maakt. Wanneer de auteursrechthebbende in de toekomst op basis van deze techniek wel toe in staat is de licentienemer te observeren dan zal hij dit binnen de kaders van de dan geldende regelgeving moeten doen.

en het privacyrechtelijk vergelijkbare overwegingen betreft, zal naar Belgisch recht slechts kort worden ingegaan op de vraag wanneer er sprake is van onrechtmatig verkregen bewijs.

5.3.2.1 Nederland

Voor het verwerken en gebruiken van persoonsgegevens bij watermerken bestaat in Nederland geen specifieke wettelijke grondslag. Dat betekent dat voor de beoordeling van de rechtmatigheid van de verwerking van deze gegevens nagegaan moet worden of bij het verwerken ervan in strijd gehandeld is met de algemene regels inzake de Wet bescherming persoonsgegevens (Wbp).[102] Op grond van deze wet moeten persoonsgegevens zorgvuldig en in overeenstemming met de wet op een behoorlijke wijze worden verwerkt.[103] Dat betekent onder meer dat persoonsgegevens op grond van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden dienen te worden verzameld en enkel verwerkt mogen worden als deze gelet op de doeleinden waarvoor ze worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.[104] Voor watermerken is het van belang dat iedere verwerking gebaseerd moet zijn op een zogenoemde verwerkingsgrondslag.[105]

De nadruk in deze paragraaf zal dan ook liggen op verwerkingsgrondslagen die bij watermerken een rol kunnen spelen. Bij het verwerken van gegevens is verder van belang dat de verwerking alleen is toegestaan zolang dit verenigbaar is met het oorspronkelijke doel van de gegevensverwerking. Een van de belangrijke beginselen in de Wbp is het informeren van de betrokkene (potentiële licentienemer) als uitwerking van het transparantiebeginsel.[106] Dit betekent dat het uitgangspunt moet zijn dat de betrokkene op de hoogte wordt gesteld van het feit dat zijn gegevens worden verwerkt op het moment dat die gegevens bij de betrokkene worden verkregen. Voor de potentiële licentienemer betekent dit dat hem duidelijk moet zijn gemaakt dat zijn gegevens worden verwerkt en dat deze gegevensverwerking mede tot doel heeft om het recht van intellectuele eigendom te handhaven.

De Wbp stelt transparantie voorop. Niettemin is het onder omstandigheden ook mogelijk om gegevens heimelijk te verwerken, bijvoorbeeld wanneer dit nodig is in het kader van opsporing. Wanneer er sprake is van heimelijke verwerking zoals onder meer bij heimelijke cameratoezicht dan moet de verwerking bij het Cbp worden gemeld.[107] Het Cbp toetst dan in een voorafgaand onderzoek de rechtmatigheid van de verwerking in verband met de

[102] Zie par. 5.3. In Nederland verder uitgewerkt in de Wet bescherming persoonsgegevens (Wbp) en binnenkort in de nog te verwachten Privacy-Verordening. Schenden van de Wbp kan onder omstandigheden ook leiden tot onderzoek van de toezichthouder. Tijdens de zaak bij het Hof Amsterdam 13 juli 2006, ECLI:NL:GHAMS: 2006:AY3854, CR 2006, 168 m. nt. N.M. Wisman (Brein/Kazaa) startte het Cbp een onderzoek n.a.v. het schenden van inlichtingenplicht, o.v. 4.10.
[103] Art. 6 Wbp.
[104] Zie art. 7 en 11 Wbp.
[105] Art. 8 Wbp.
[106] Van de informatieplicht kan op grond van artikel 43 Wbp in uitzonderingsgevallen worden afgezien.
[107] Om de betrokkene toch enige bescherming te bieden dient de verantwoordelijke het CBP in de gelegenheid te stellen een voorafgaand onderzoek in stellen waarin het CBP de rechtmatigheid toetst van de verwerking in verband met de bijzondere risico's die een heimelijke waarneming met zich brengt.

bijzondere risico's die een heimelijke waarneming met zich meebrengt. Dit betekent voor de inzet van het watermerk dat de rechthebbende in beginsel twee keuzes heeft. Of hij informeert de potentiële licentienemer over de mogelijke verwerkingen van zijn persoonsgegevens en geeft hem daarmee de kans om te bepalen of hij die gegevensverwerking en daarmee de aankoop van een product wenselijk acht of niet. Of hij informeert de potentiële licentienemer niet en zal de heimelijke verwerking van de persoonsgegevens moeten melden bij het Cbp die dan een rechtmatigheidscontrole uitvoert.

Tot slot kan er nog op worden gewezen dat de rechthebbende de verwerking ook bij het Cbp moet melden wanneer hij de licentienemer wel informeert over het gebruik van zijn gegevens in het watermerk. In dat geval zal het Cbp in beginsel geen rechtmatigheidscontrole uitvoeren. Verder zal de rechthebbende zich ook moeten houden aan andere voorwaarden die de Wbp stelt aan het zorgvuldig verwerken van persoonsgegevens, zoals de bewaartermijn, het treffen van passende technische en organisatorische maatregelen ter bescherming van persoonsgegevens of het melden van de verwerking van persoonsgegevens bij het Cbp.[108] Deze omstandigheden worden verder buiten beschouwing gelaten omdat zij in beginsel niet specifiek zijn voor het werken met watermerken.

De Hoge Raad heeft in een aantal arresten duidelijk gemaakt dat een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer in beginsel een onrechtmatige daad oplevert.[109] De aanwezigheid van een rechtvaardigingsgrond kan aan een inbreuk echter het onrechtmatige karakter ontnemen. Of daarvan sprake is kan volgens de Hoge Raad slechts worden beoordeeld in het licht van de omstandigheden van het geval door de ernst van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer af te wegen tegen de belangen die met de inbreuk makende handelingen redelijkerwijs kunnen worden gediend.

Inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer

In relatie tot watermerken ligt een schending ten aanzien van het (privacy)recht het meest voor de hand wanneer de rechthebbende, bij het verwerken van persoonsgegevens van de licentienemer in het watermerk, handelt in strijd met de Wet bescherming persoonsgegevens. Daarbij kunnen in beginsel twee gevallen worden onderscheiden. Ten eerste het geval dat de rechthebbende zelf zijn werken met watermerk aanbiedt via zijn eigen website en zelf de gegevens daarvan verwerkt. In het tweede geval biedt de rechthebbende niet zelf maar via een derde, zoals een webwinkel, hotel of bioscoop, zijn werken aan. Het laatste geval zal zich in de praktijk het meeste voordoen. Het is ook denkbaar dat een andere organisatie zoals een

[108] Vgl. Hof Leeuwarden 5 december 2011, ECLI:NL:GHLEE:2011:BU6824, ov. 23 die in een strafzaak het overschrijden van de bewaringstermijn voldoende acht om de verkrijging van ANPR-informatie onrechtmatig te achtten. Zie in het strafrecht verder ook de serie arresten voorafgaand aan HR 11 november 2014 ECLI:NL:HR: 2014:3142, JIN 2014/228 m.nt. C.J.A. de Bruijn.

[109] HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, NJ 1987/928 m.nt. E.A. Alkema (Grumbock/Van der Kaaij; Edamse bijstandsmoeder), ov. 4.4.; HR 31 mei 2002, ECLI:NL:HR:2002:AD9609, NJ 2003/589 m.nt. J.B.M. Vranken, ov. 3.5.2; meer recentelijk herhaalt in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.1

Thrusted Third Party (TTP) de persoonsgegevens verwerkt. In al deze gevallen moeten partijen die de gegevens verwerken zich houden aan de regels die de Wbp aan de verwerking stelt en kan overtreding van die regels ertoe leiden dat de persoonsgegevens die onrechtmatig worden verwerkt als onrechtmatig verkregen bewijs worden gekwalificeerd.

Het verwerken van persoonsgegevens dient overeenkomstig de bepalingen van de Wbp plaats te vinden op basis van een zogenoemde verwerkingsgrondslag. Bij het sluiten van de overeenkomst beschikt de verkoper reeds over persoonsgegevens van de licentienemer om de overeenkomst uit te kunnen voeren, zoals de naam en het rekeningnummer van de licentienemer.[110] De verkoper mag deze gegevens voor dat doel verwerken op grond van artikel 8, onder b Wbp (uitvoering van de overeenkomst). Het verwerken van dezelfde gegevens in het watermerk ten behoeve van het handhaven van auteursrechten is in beginsel een ander doel dan het uitvoeren van de overeenkomst en vereist om die reden een eigen grondslag. In de praktijk zal ten aanzien van de vraag naar de onrechtmatigheid dan ook voornamelijk een rol spelen op welke grond en onder welke voorwaarden deze gegevens in het watermerk verwerkt kunnen worden.

De vraag naar de verwerkingsgrondslag voor watermerken werd actueel toen verschillende websites meldden dat webwinkels die e-boeken leveren via het distributieplatform eBoekhuis zich er via een overeenkomst met CB toe verplichten, om op verzoek van de Stichting Brein (hierna: Brein) klantgegevens te verstrekken zodat Stichting Brein tot handhaving over kan gaan.[111] Op basis van deze overeenkomst zou de webwinkel de aankoopinformatie ten minste twee jaar moeten bewaren.[112] Tevens zouden de webwinkels verplicht zijn om consumenten tijdens de aankoop van een e-boek met watermerk te wijzen op het feit dat informatie van klanten bewaard wordt en bij een vermoeden van misbruik mogelijk wordt doorgespeeld naar derden. Hiermee kiest dit deel van de boekenbranche niet voor de weg van heimelijkheid maar van transparantie. Daarbij zal zonder meer een rol hebben gespeeld dat het kenbaar maken van (watermerk)beveiliging ook een preventieve werking kan hebben.[113] Een voorbeeld van het informeren van klanten is de melding die Bol.com maakt op haar website onder het kopje ‘Ebooks beveiliging’: ‘Het illegaal kopiëren van ebooks vinden wij vervelend. Auteurs en uitgevers zijn immers afhankelijk van de inkomsten van ebooks. De ebooks die wij verkopen zijn daarom voorzien van een zogenaamde watermerkbeveiliging.

[110] In par. 2.3.3 is reeds duidelijk geworden dat de gegevens die in het watermerk gestopt zullen worden beperkt zullen blijven tot gegevens die de licentienemer al reeds ter beschikking heeft gesteld voor de uitvoering van de overeenkomst. Zie ook Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360, ov. 4.8: ‘[…] zijn identificeerbaar aan de hand van hun e-mailadres en de door hen opgegeven bankrekening’.
[111] Zie http://www.ereaders.nl/09081301_inzet_brein_juridisch_afgedekt_in_nieuw_ebookdistributiecontract.
Zie voor een korte bespreking ook Arnoud Engelfriet (AE 5993). In totaal voorziet CB ongeveer 2500 winkels in Nederland en België van boeken, maar het in onduidelijk hoeveel winkels vallen onder deze regeling. Zie voor het belang van het contract o.m. vzr. Rb. Amsterdam 28 januari 2015, IEF 14603 (Belirex/UPC) die overwoog (4.5) dat de Wbp zich niet verzet tegen afgifte maar dat dit niet betekent dat UPC verplicht is om tot afgifte over te gaan. De rechter constateert dat er geen overeenkomst tussen partijen bestaat op grond waarvan UPC daartoe gehouden zou zijn.
[112] Dit duidt erop dat deze rechthebbenden vooral de eerste twee jaren de bescherming van belang vinden.
[113] Zie o.m. par. 3.2.2.

Het watermerk heeft zichtbare en onzichtbare kenmerken. Zo worden pagina's van de ebooks voorzien van unieke gegevens. We kunnen zo nagaan wie het boek heeft besteld. Wanneer ebooks illegaal worden gekopieerd, kunnen we een contractuele of wettelijke plicht hebben om te vertellen wie de koper van de originele ebooks is.'[114] Deze melding komt overigens niet duidelijk naar voren wanneer je een webpagina bezoekt waarop een gewatermerkt e-boek wordt aangeboden.

De rechthebbende dwingt haar distributeurs door middel van het voornoemde contract om Wbp na te leven en zorgt er daarmee voor dat hij de kans verkleint dat het watermerk in een procedure als onrechtmatig bewijs zal worden gekwalificeerd. Het gebruik van het watermerk maakt het achterhalen van de licentienemer eenvoudiger. De rechthebbende kan, wanneer hij aannemelijk kan maken dat er sprake is van inbreuk op het auteursrecht al enige tijd relevante gegevens opvragen bij derden op basis van en met inachtneming van de overige criteria uit het Lycos/Pessers-arrest.[115] Bij het beantwoorden van de Kamervragen merkt de minister tevens op dat mede gelet op een vrije toegang tot informatie en cultuur, ook de vraag van belang is of de licentienemer ook langs andere weg kennis kan nemen van het boek. Wat de minister hier precies mee bedoelt is mij niet duidelijk.[116] Betekent dit dat wanneer er geen papieren versie meer verkrijgbaar is, de rechthebbende niet langer de verwerking van persoonsgegevens als voorwaarde aan een verkoop mag stellen? Dit lijkt mij een onhoudbare weg. Meer voorstelbaar is het dat de minister hiermee tot uitdrukking heeft willen brengen, dat vrije toegang tot informatie en cultuur een factor is die meeweegt bij het beoordelen van een rechtsvraag, zoals dit ook het geval was in de eerder besproken Sabam-zaak.[117]

Wanneer rechthebbenden bij de inzet van watermerken kiezen voor transparantie dan is ondubbelzinnige toestemming van de persoon van wie de gegevens worden verwerkt de meest voor de hand liggende verwerkingsgrond (artikel 8 onder a Wbp).[118] Dit zou betekenen dat de licentienemer een expliciete mededeling of actieve handeling moet verrichten waaruit de toestemming blijkt en bovendien moet deze toestemming voldoende specifiek zijn. Er zal duidelijk gemaakt moeten worden dat de gegevensverwerking gebruikt wordt voor handhaving van auteursrecht (doelomschrijving) en in dat kader ook doorgifte aan derden zoals Brein mogelijk is. Immers ook voor de doorgifte aan Brein moet toestemming worden gevraagd. In de regel zal dat gebeuren door een apart vakje waarin de licentienemer hier specifiek toestemming voor geeft. Wanneer de winkel deze voorzieningen niet treft dan is

[114] http://www.bol.com/nl/m/voorwaarden/privacy-policy/index.html. Laatst geraadpleegd op 6-01-2015.
[115] HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers); Zie ook HvJ EU 29 januari 2008, zaak C 275/06, Jur. p. I 271 (Promusicae); HvJ EU, 19 april 2012, zaak C-461/10, (Bonnier Audio).
[116] Zie ook Engelfriet (AE 5993).
[117] Par. 5.3.1.1; HvJ EG 24 november 2011, zaak C-70/10 (Scarlet/Sabam) waarin het HvJ EU tegen de achtergrond van drie grondrechten uit het Handvest (vrijheid van ondernemerschap (art. 16), het recht op bescherming van persoonsgegevens (art. 8) en informatievrijheid (artikel 11)) de eerste kaders opgesteld naar aanleiding van de vraag of een service provider (ISP) kan worden verplicht een filter in te voeren.
[118] Zie ook de minister van Veiligheid en Justitie in antwoord op kamervragen. Zie Aanhangsel van de Handelingen 2013-2014, 116 voor zowel de vragen als de antwoorden van de minister.

hiermee nog niet gezegd dat hij ook in strijd met de Wbp handelt.[119] Toestemming levert weliswaar de meest voor de hand liggende verwerkingsgrond op, maar zij vormt niet de enige verwerkingsgrond.

De tweede grond waarop een beroep kan worden gedaan is de rechtvaardigingsgrond van artikel 8, onder b Wbp waarin gegevensverwerking is toegestaan in het kader van de uitvoering van een overeenkomst waarbij de licentienemer zelf betrokken is. De rechtvaardigingsgrond bestaat wanneer 'gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst'. Het gaat hier volgens de MvT om handelingen die op verzoek van de betrokkene worden verricht om de overeenkomst te kunnen sluiten.[120] In de regel geldt dat een dergelijke verwerking alleen is toegestaan wanneer de verwerking nodig is om de overeenkomst uit te kunnen voeren. Bijvoorbeeld omdat de gegevens verwerkt moeten worden om een online besteld product bij iemand bezorgd te krijgen. Om die reden zal het verwerken van gegevens in watermerken niet snel kunnen plaatsvinden op deze grondslag. De gegevensverwerking die voortvloeit uit de contractuele eis dat e-boeken van watermerken moeten worden voorzien voordat deze mogen worden verkocht kunnen weliswaar als noodzakelijke precontractuele stappen worden gezien om de uiteindelijke overeenkomst te kunnen sluiten, maar kunnen bezwaarlijk worden aangemerkt als handelingen die op verzoek van de betrokkene worden verricht. Deze handelingen beogen immers het gerechtvaardigd belang van de rechthebbende te beschermen en niet die van de betrokkene. De gegevensverwerkingen die in het kader van deze handelingen plaatsvinden zouden eventueel nog kunnen worden gerechtvaardigd door artikel 8, onder f Wbp.

Tot slot kan er naast toestemming en uitvoering van de overeenkomst ook nog een verwerkingsgrond worden gevonden wanneer de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert (artikel 8 onder f Wbp). De noodzaak en het rechtvaardigde belang zou in dit geval gevonden kunnen worden in handhaving van het auteursrecht. De minister wijst erop dat webwinkels zelf een belang kunnen hebben bij het bewaren van klantgegevens omdat de gratis distributie van e-boeken volgens hem ten koste kan gaan van hun verkoop.[121] In dat kader kunnen zij ook afspraken maken met derden. De noodzakelijkheid van de gegevensverwerking moet vervolgens nog worden beoordeeld in het licht van de proportionaliteit en subsidiariteit. Bij de beoordeling van de proportionaliteit dienen de inzet van de bevoegdheid

[119] Een winkel die een overeenkomst heeft gesloten met CB handelt in beginsel dan wel in strijd met de bepaligen uit de tussen hem en CB gesloten overeenkomst.
[120] MvT, II, nr. 3 p. 81.
[121] Indien winkels menen dat zij door het economisch overwicht door een derde worden gedwongen om bepaalde contractsvoorwaarden te accepteren, kunnen zij volgens de minister de toezichthouder vragen om te beoordelen of er misbruik wordt gemaakt van een machtspositie.

en de mate waarin de gegevens worden verwerkt te worden afgewogen tegen het te bereiken doel van in dit geval handhaving. Bij de toets van subsidiariteit dient de vraag te worden beantwoord of er ook minder vergaande middelen zijn om het doel te bereiken. Een beroep op deze (vangnet)bepaling zou naar mijn mening moeten falen wanneer de rechthebbende de licentienemer niet heeft ingelicht over de gegevensverwerking in het watermerk en het doel van de gegevensverwerking. Door het informeren van de licentienemer had immers gekozen kunnen worden voor een methode die minder inbreuk maakt op de privacy van de licentienemer. Dat zou slechts anders kunnen zijn wanneer zou blijken dat heimelijk aangebrachte watermerken aanzienlijk beter werken.[122] Daarnaast zou deze bepaling niet ten voordele mogen strekken van de rechthebbende wanneer deze zelf nalaat om een eenvoudige en goedkope maatregel te treffen, zoals het informeren van de licentienemer.

Samenvattend kan worden gesteld dat wanneer de persoonsgegevens van de licentienemer in het watermerk worden opgenomen, de licentienemer zowel moet worden geïnformeerd over de verwerking als over het doel ervan, inclusief eventuele doorgifte van zijn gegevens. Het nalaten hiervan kan leiden tot het oordeel dat er in strijd gehandeld is met de Wbp en daarmee inbreuk is gepleegd ten aanzien van de privacy van in dit geval de licentienemer. Voor de volledigheid kan er nog op worden gewezen dat de Wbp nog in de mogelijkheid voorziet dat van de informatieplicht kan worden afgeweken voor zover dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.[123] Zoals eerder besproken zal het Cbp dan in een voorafgaand onderzoek de rechtmatigheid van de verwerking toetsen in verband met de bijzondere risico's die een heimelijke waarneming met zich brengt. In een rechtszaak zal de rechter evenals bij een beroep op artikel 8 onder f Wbp de noodzakelijkheid van de gegevensverwerking beoordelen in het licht van de proportionaliteit en subsidiariteit.[124]

Rechtvaardiging: ernst van de inbreuk

Wanneer de rechter tot de conclusie komt dat de rechthebbende zonder daartoe gerechtigd te zijn gegevens van de licentienemer in het watermerk heeft verwerkt is er in beginsel sprake van een onrechtmatige daad. Het recht op privacy is geen absoluut recht. De aanwezigheid van een rechtvaardigingsgrond kan derhalve aan een inbreuk het onrechtmatige karakter ontnemen. Of daarvan sprake is kan volgens de Hoge Raad slechts worden beoordeeld in het licht van de omstandigheden van het geval door de ernst van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer af te wegen tegen de belangen die met de inbreuk makende handelingen redelijkerwijs kunnen worden gediend.[125] Bij watermerken zal

[122] Onderzoek naar die gegevens zijn mij op dit moment onbekend.
[123] Art. 42 onder b Wbp.
[124] Zie o.m. Rb. Rotterdam 27 maart 2013, ECLI:NL:RBROT:2013:BZ6071, ov. 4.15 en de tekst hierna ten aanzien van heimelijk cameratoezicht.
[125] HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, NJ 1987/928 m.nt. E.A. Alkema (Grumbock/Van der Kaaij; Edamse bijstandsmoeder), ov. 4.4.; HR 31 mei 2002, ECLI:NL:HR:2002:AD9609, NJ 2003/589 m.nt. J.B.M. Vranken, ov. 3.5.2.; meer recentelijk herhaalt in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.1. Zie in het

de rechter een afweging moeten maken tussen enerzijds het belang van de licentienemer bij eerbiediging van zijn persoonlijke levenssfeer en anderzijds het belang van de rechthebbende bij het beschermen van zijn intellectuele eigendom. In dit verband kunnen de aard en inhoud van de gesloten overeenkomst mede van belang zijn.[126] Bij de beoordeling van de ernst van de inbreuk kan ook de aard en de mate van intimiteit van de informatie van groot gewicht zijn.[127] Bij het verwerken van eenvoudige en niet-bijzondere persoonsgegevens, zoals de NAW-gegevens zal de ernst van de inbreuk mede vanwege de aard en zeer beperkte mate van intimiteit gering worden geacht.

Voor de beoordeling of bij watermerken een succesvol beroep kan worden gedaan op een rechtvaardigingsgrond dient als uitgangspunt te worden genomen dat de rechthebbende zich niet gehouden heeft aan de regels die de Wbp stelt ten aanzien van de verwerking van persoonsgegevens teneinde onder meer de licentienemer te beschermen tegen onnodige inbreuken op de persoonlijke levenssfeer. In de kern ligt het probleem van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer van de licentienemer bij watermerken bij het schenden van de informatieplicht of het kenbaarheidsvereiste. Een toetsingskader daarvoor kan worden gevonden in de jurisprudentie ten aanzien van verborgen cameratoezicht waarin duidelijk is geworden dat wanneer een partij een gerechtvaardigd belang heeft, het gebruik van die gegevens onder voorwaarden niet geldt als onrechtmatig verkregen bewijs.[128]

In zowel de zaak L./Wennekes Lederwaren bij de Hoge Raad als in de zaak Köpke/Duitsland bij het EHRM doet zich de situatie voor dat een medewerker wordt verdacht van verduistering. In beide zaken beroept de medewerker zich op het recht op privacy omdat er zonder zijn medeweten een camera was geplaatst. In het arrest L./Wennekes Lederwaren komt de Hoge Raad tot het oordeel dat voor het beantwoorden van de vraag of er sprake is van een ongeoorloofde inbreuk op het privacyrecht, het onder meer van belang is dat er een concreet vermoeden bestond dat een van de werknemers zich schuldig maakte aan strafbare feiten, welk vermoeden, anders dan met gebruikmaking van een verborgen camera niet zou kunnen worden gestaafd.[129] Ook het Europees Hof voor de Rechten van de Mens (EHRM) kwam tot vergelijkbare overwegingen.[130] Het EHRM is in deze zaak onder verwijzing naar eerder gewezen arresten nagegaan of de Duitse rechter voldoende aandacht heeft gehad voor specificiteit van de doelstelling, de proportionaliteit en de subsidiariteit van de ingreep in het privéleven van de oorspronkelijke gedaagde. Het Hof vond geen inbreuk op artikel 8 EVRM,

licht van het intellectueel eigendomsrecht o.m. HvJ EU 19 april 2012, C-416/10, ECLI:EU:C:2012:219 (Bonnier Audio); HvJ EG 29 januari 2008, zaak C-275/06 (Promusicae/Telefónica).

[126] HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.1.

[127] HR 16 oktober 1987, ECLI:NL:HR:1987:AC9997, NJ 1988, 850, m.nt EAA (Dreissen/Van Gelder), ov. 3.4.3. onder verwijzing naar de MvT bij artikel 10 Gw; Bijl. Hand. II, 1975–1976, 13 872, nrs. 1–5, p. 41.

[128] HR 27 april 2001, ECLI:NL:HR:2001:AB1347, NJ 2001/421, m.nt. PAS (L/Wennekes Lederwaren); EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, NJ 2011/566 m.nt. EJD (Köpke/Duitsland). Zie voor het heimelijke karakter en de wederrechtelijkheid bij cameratoezicht ook de Minister Handelingen Eerste Kamer, 2002-2003, nr. 23, pag. 736-742; Nadere Memorie van Antwoord, Eerste Kamer, 2002-2003, nr. 57c.

[129] HR 27 april 2001, ECLI:NL:HR:2001:AB1347, NJ 2001/421, m.nt. PAS (L/Wennekes Lederwaren).

[130] EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, NJ 2011/566 m.nt. EJD (Köpke/Duitsland).

nu de Duitse rechter rekening had gehouden met het feit dat de werkneemster haar werk op basis van het contract op die plaats moest uitvoeren en daar niet onderuit kon, de toezichtsmaatregel is genomen naar aanleiding van een specifiek vermoeden van onrechtmatig gedrag van een werknemer, de waarneming noodzakelijk was om bewijs te verkrijgen, het toezicht beperkt was in tijd en beperkt tot een publiek toegankelijk gebied rondom de kassa van de drankafdeling. Bovendien had de Duitse rechter rekening gehouden met het feit dat de toegang tot het beeldmateriaal beperkt was gebleven tot de bedrijfsrecherche en de stafleden van de werkgever. De beelden zijn verder ook alleen gebruikt als bewijs in deze ontslagprocedure en met het bewaren daarvan is een eerlijke rechtsbedeling gediend. De Duitse rechter had ook in zijn beslissing gewicht toegekend aan het belang van een betrouwbare medewerker en een afweging gemaakt ten aanzien van andere minder ingrijpende maatregelen. Het EHRM sluit echter niet uit dat er in de toekomst mogelijk een ander gewicht aan de belangen van betrokkenen moeten worden toegekend gelet op de mate waarin inbreuken op het privéleven mogelijk worden gemaakt door nieuwe, steeds verder ontwikkelde technologieën.[131]

Beide arresten laten zien dat de ernst van de fraude met zich mee kan brengen dat er sprake kan zijn van een rechtvaardigingsgrond wanneer er een concreet vermoeden bestaat dat een werknemer zich schuldig maakt aan strafbare feiten, welk vermoeden, anders dan met gebruikmaking van een verborgen camera niet zou kunnen worden bevestigd.[132] Anders dan bij verborgen cameratoezicht kan bij watermerken niet worden gezegd dat de (toezichts)maatregel is genomen naar aanleiding van een concreet vermoeden van onrechtmatig gedrag van een licentienemer.[133] Watermerken met daarin de gegevens van de licentienemer worden immers aangebracht zonder dat er sprake is van een specifiek vermoeden. Het concrete vermoeden, van een in beginsel ook strafbaar feit, ontstaat pas op het moment dat het werk op internet is aangetroffen en de rechthebbende heeft vastgesteld dat er sprake is van inbreuk op het auteursrecht. Om de vraag te kunnen beantwoorden of het vermoeden niet anders dan met gebruikmaking van een watermerk zou kunnen worden bevestigd dient eerst te worden gekeken naar alternatieven in het hele veld van de opsporing. Dat het anders kan blijkt uit het feit dat ook voor de introductie van het watermerk opsporing van uploaders en downloaders mogelijk was. Watermerken maken de opsporing daarentegen eenvoudiger door tenminste een spoor te bieden van waaruit de opsporing kan beginnen. Het watermerk lijkt daarmee wel een beter handhavings- en/of opsporingsmiddel dan eerder

[131] ‘The competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies.’
[132] Hoewel het in beide arresten gaat over een geschil tussen een werkgever en werknemer moet daarin m.i. geen bijzondere rol worden toegekend aan de in beginsel bijzondere verhouding. In beide arresten speelt de bijzondere verhouding immers geen rol, anders dan het belang van een betrouwbare medewerker. Die verhouding is echter niet anders dan tussen partijen die nakoming van de overeenkomst mogen verwachten.
[133] Vgl. ook Hof ‘s-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465, ov. 37, bekrachtigd in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.4.2.

gebruikte technieken zoals het volgen van een IP-adres.[134] In het domein van Digital Rights Management (DRM) zijn verder vele alternatieven denkbaar: van kopieerbeveiliging tot het zichtbaar aanbrengen van de naam van de licentienemer.[135] Om licentienemers die in strijd met de gesloten licentieovereenkomst werken op internet plaatsen te kunnen traceren zijn niettemin meer technieken denkbaar. Bij iedere techniek waarbij op een moment persoonsgegevens van de gebruiker worden verwerkt teneinde de licentienemer te kunnen traceren speelt uiteindelijk dezelfde problematiek een rol: het zorgvuldig omgaan met de persoonsgegevens van de licentienemer. Hoewel de ernst van de inbreuk op het privacyrecht van de licentienemer in dit geval beperkt is gebleven tot het heimelijk verwerken van eenvoudige persoonsgegevens in een watermerk bestond er bij de rechthebbende ten tijde van het verwerken van de persoonsgegevens in het watermerk geen concreet vermoeden van onrechtmatig gedrag van een licentienemer. Bovendien kan de rechthebbende door toestemming te vragen ook kiezen voor een methode die geen inbreuk maakt op de privacyrechten van de licentienemer. Er is dan ook geen reden voor de rechthebbende om in strijd te handelen met de voorwaarden die de Wbp aan het verwerken van gegevens stelt.[136] Wanneer hij dit nalaat handelt hij onrechtmatig en is een rechtvaardigingsgrond naar mijn mening niet snel meer denkbaar.

In de zaak Achmea/Rijnberg deed zich de situatie voor dat een verzekeraar in strijd handelde met de door het Verbond van Verzekeraars opgestelde Gedragscode.[137] De vraag die zich bij de vraag naar het onrechtmatige karakter voordeed was kort gezegd of er ruimte is voor een zelfstandige belangenafweging wanneer er in strijd gehandeld is met de door het Verbond van Verzekeraars opgestelde Gedragscode. De Hoge Raad overweegt dat wanneer er met de Gedragscode invulling is gegeven aan een belangenafweging die nodig is om te kunnen bepalen of er sprake is van een onrechtmatige inbreuk op de persoonlijke levenssfeer van de verzekerde, er gelet op de inhoud en opzet van de Gedragscode tot uitgangspunt kan worden genomen dat indien een verzekeraar in strijd met de code handelt, er sprake is van onrechtmatig verkregen bewijs. Het hof kwam eerder tot het oordeel dat er niet aan de vereisten van de Gedragscode was voldaan voor het instellen van een persoonlijk onderzoek en dat daarmee gegeven is dat er sprake is van een inbreuk op de persoonlijke levenssfeer van de verzekerde. De Hoge Raad acht dit oordeel niet onbegrijpelijk.[138] Met andere woorden wanneer in de gedragscode reeds een belangenafweging heeft plaatsgevonden in overeenstemming met het geldende recht dan zal het handelen in strijd met die gedragscode er

[134] Vgl. Vzr. Rb. Amsterdam 28 januari 2015, IEF 14603 (Belirex/UPC), ov. 4.9 waarin de rechter stelt dat IP-adressen veelal verwijzen naar een router die voor meerdere gebruikers een internetverbinding mogelijk maken waardoor het niet duidelijk wordt wie zich schuldig heeft gemaakt aan illegaal downloaden.
[135] Zie par. 3.2.1 en voor een overzicht van technische voorzieningen o.m. de dissertatie van Koelman (2003).
[136] Hiermee is niet gezegd dat heimelijke verwerking altijd is uitgesloten. Zoals eerder in de tekst is aangegeven blijft dat mogelijk, mits daarvan melding is gemaakt bij het Cbp en het watermerk de rechtmatigheidstoets van het Cbp doorstaat.
[137] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg); Hof ‘s-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465 (Achmea/Rijnberg).
[138] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.3.2.

in de regel tevens toe leiden dat er sprake is van onrechtmatig verkregen bewijs.[139] Wanneer schending van een dergelijke gedragscode eenmaal vaststaat is kans op een succesvol beroep op de aanwezigheid van een rechtvaardigingsgrond klein.[140] Voor watermerken bestaat erop dit moment geen vergelijkbare gedragscode.[141]

Lubbers en Oskam vinden de bewoordingen van de Hoge Raad echter wel erg ruim op dit punt.[142] De Gedragscode bevat, zo stellen zij, naast gronden die aanleiding kunnen geven om een persoonlijk onderzoek te starten en de vereisten van proportionaliteit en subsidiariteit, ook andere regels die minder of geen betrekking hebben op de beslissing om persoonlijk onderzoek te starten. Zij stellen de vraag wat bijvoorbeeld de consequentie is indien de verzekeraar in strijd met de Gedragscode de benadeelde niet achteraf over het verrichte onderzoek informeert. Het lijkt hen vrij vergaand om ook dan te concluderen dat sprake is van een onrechtmatige inbreuk op de persoonlijke levenssfeer van betrokkene. Ik deel deze mening niet, omdat ik niet kan inzien waarom de verzekeraar zich niet aan de eigen gedragsregels zou moeten houden. Men zou kunnen stellen dat het geen recht doet aan de beperkte inbreuk die er dan wordt gemaakt. Daar kan echter even goed tegenover worden gesteld dat het geen recht doet aan de gestelde regel als die toch zonder consequenties overtreden kan worden. Zoals zij zelf in hun annotatie stellen heeft het Verbond van Verzekeraars de Gedragscode Persoonlijk Onderzoek geïntroduceerd om nader invulling te geven aan de belangenafweging tussen enerzijds recht op privacy van de verzekerde en anderzijds voorkomen dat misbruik wordt gemaakt van de verzekering. Het geheel van regels maakt onderdeel uit van die gemaakte belangenafweging. Daarbij past het in beginsel niet om enkele regels buiten toepassing te verklaren. Ik zie daarom niet snel een reden om bepaalde voorwaarden buiten toepassing te verklaren. Er zijn onder omstandigheden vanzelfsprekend altijd uitzonderingen denkbaar. De Hoge Raad laat daar ook ruimte voor als zij tot het oordeel komt dat wanneer een verzekeraar in strijd met de Gedragscode handelt, dat in beginsel een onrechtmatige inbreuk op de persoonlijke levenssfeer van de verzekerde oplevert. De Hoge Raad laat ruimte aan de verzekeraar om zelf bijkomende omstandigheden aan te voeren die een inbreuk wel zouden rechtvaardigen. Bovendien leidt een oordeel dat er sprake is van onrechtmatig verkregen bewijs nog niet automatisch tot het oordeel dat het bewijs moet worden uitgesloten, waardoor ook niet kan worden gesteld dat de verzekeraar onevenredig hard zou worden geraakt. Ook daarom is er weinig reden om aan te nemen dat verzekeraars zich niet aan alle voorwaarden van de Gedragscode zouden moeten houden.

[139] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.2.1: ‘In cassatie is dan ook terecht niet in geschil dat de beslissing van Interpolis om een persoonlijk onderzoek te doen uitvoeren, door het hof aan de in de Gedragscode uitgewerkte beginselen van proportionaliteit en subsidiariteit diende te worden getoetst’. Zie Menting 2015 die erop wijst dat de Hoge Raad lijkt te suggereren dat de private aard van de regels geen drempel (meer) vormt voor hun juridische relevantie. Een stap waar de lagere rechtspraak al vaker toe neigt wanneer zij hiertoe de kans krijgen van partijen (die deze regelgeving ter sprake moeten brengen).
[140] Zie ook Lubbers en Oskam in hun noot onder HR 18 april 2014, ECLI:NL:HR:2014:942, JA 2014/65.
[141] De eerder besproken ‘Privacy Principles for Digital Watermarking’ (par. 5.3.1.2) zou model kunnen staan voor een dergelijke gedragscode.
[142] Lubbers en Oskam in hun noot onder het arrest van HR 18 april 2014 ECLI:NL:HR:2014:942, JA 2014/65.

Tot slot kan er nog op worden gewezen dat een andere rechtvaardigingsgrond kan worden gevonden in de omstandigheid dat in beginsel bewijsmateriaal dat op onrechtmatige wijze is verkregen door een ander dan de procespartij die het wil gebruiken, nog niet met zich meebrengt dat dit materiaal ook door die procespartij onrechtmatig is verkregen.[143] Er is echter geen reden om aan te nemen dat de rechthebbende zich bij de verkrijging van het bewijs kan beroepen op de omstandigheid dat niet hij maar bijvoorbeeld de webwinkel de gegevens ten onrechte in het watermerk heeft verwerkt en het bewijs om die reden niet kan worden uitgesloten. In het geval als hiervoor bedoeld is het van belang dat de onrechtmatige verkrijging aan de rechthebbende zelf kan worden toegerekend.[144] De distributeur of webwinkel zal immers middels een overeenkomst gehouden zijn het watermerk als handhavingsmiddel te gebruiken.[145] Tevens moet worden voorkomen dat partijen in staat worden gesteld om bewijs wit te wassen.

In de praktijk zullen, evenals het eerder genoemde voorbeeld van e-boeken, overeenkomsten worden gesloten tussen aanbieders van de producten en de rechthebbenden. In het licht van de eerder genoemde overeenkomst is aannemelijk geworden dat er voldoende aandacht is voor het verwerken van de persoonsgegevens en het informeren van licentienemers over het gebruik van watermerken. Daar komt bij dat toezichthouders de rechthebbende ook kunnen confronteren met onderzoek, handhaving en forse boetes wanneer zij in strijd handelen met de normen die de persoonlijke levenssfeer betreffen. Ook hierin kan een reden gevonden worden om zorgvuldig om te gaan met persoonsgegevens. Er is dan ook weinig reden om aan te nemen dat de vraag naar de rechtmatigheid van het watermerk als bewijsmiddel zich in de praktijk snel zal voordoen. Wanneer de rechthebbende desalniettemin niet handelt overeenkomstig de eisen die de Wbp stelt aan de verwerking van persoonsgegevens, dan zal de rechter tot het oordeel moeten komen dat er sprake is van onrechtmatig verkregen bewijs.

5.3.2.2 België

Om naar Belgisch recht te bepalen of bewijs geoorloofd is moet bepaald worden of het bewijs naar haar aard rechtmatig is en of het bewijs op een rechtmatige wijze is verkregen.[146] Bewijsmiddelen die uit hun aard onrechtmatig zijn, zijn ook naar Belgisch civiel recht steeds ongeoorloofd.[147] In beginsel wordt een bewijsmiddel als onrechtmatig beschouwd wanneer het naar zijn aard neerkomt op het schenden van vertrouwelijkheid, valsheid of strijdigheid met de openbare orde en de goede zeden.[148] Bij vertrouwelijkheid kan in relatie tot het watermerk met name in de opsporingsfase als eerste worden gedacht aan het recht op

[143] Vgl. HR 7 februari 1992, ECLI:NL:HR:1992:ZC0500, NJ 1993/78, m.nt. Snijders; HR 11 juli 2014 ECLI:NL:HR:2014:1632, JIN 2014/175 m.nt. P.C.M. Kemp, JBPr 2014/52 m.nt. M. Kremer, ov. 3.4.1.
[144] Zie art. 6:162 lid 3 BW.
[145] Zie de eerder besproken overeenkomst tussen de aanbieders van e-boeken en CB (par. 5.3.2.1).
[146] Mougenot 2011, p. 242; Van Kildonck 2010, p. 180; Mougenot 2009, p. 106-109; Wagner 2008; Hendrickx 2006, p. 671; Allemeersch en Schollen 2002, p. 41;
[147] Allemeersch & Schollen 2002, p. 60; Allemeersch & Van Orshoven 2011, p. 73; Laenens 2012, p. 550.
[148] Allemeersch & Schollen 2002, p. 41; De Corte 2003, p. 809; Hendrickx 2006, p. 671; Van Kildonck 2010, p. 180; Laenens 2012, p. 550.

privacy.[149] Aan het louter schenden van zorgvuldigheidsnormen wordt in de literatuur in relatie tot het recht op bewijslevering minder gewicht toegekend.[150] Dit geldt ook voor die gevallen waarin bepalingen uit een contract worden geschonden, bijvoorbeeld bij het schenden van de geheimhoudings- dan wel vertrouwelijkheidsplicht.[151] Bewijsmiddelen die zijn verkregen door een onrechtmatige daad of zijn verzameld in strijd met de privacyrechten van de licentienemer zijn op die grond onrechtmatig verkregen.[152] Samenvattend is onrechtmatig bewijs uit zijn aard onrechtmatig en kan om die reden door niemand worden gebruikt, terwijl rechtmatig bewijs enkel niet kan worden gebruikt door de persoon die het onrechtmatig heeft verkregen, maar weer wel door de persoon die het bewijs rechtmatig in zijn bezit kreeg.[153]

Voor nu staat de vraag naar de rechtmatigheid van de verkrijging centraal. Bij watermerken gaat het, evenals naar Nederlands recht, dan om of er sprake is van schending van de privacy van de gebruiker. De rechter zal bij een beroep op inbreuk op het privacyrecht allereerst moeten vaststellen of de voorliggende situatie door specifieke wetgeving wordt geregeld.[154] Voor het verwerken en gebruiken van persoonsgegevens bij watermerken bestaat ook in België geen specifieke wettelijke grondslag. Dat betekent dat voor de beoordeling van de rechtmatigheid van de verwerking van deze gegevens, evenals naar Nederlands recht, nagegaan moet worden of bij het verwerken ervan in strijd gehandeld is met de algemene regels inzake de Wet met betrekking tot de verwerking van persoonsgegevens (WVP).[155] Deze wet komt evenals de Nederlandse Wbp voor een belangrijk deel voort uit de Europese privacyrichtlijn (95/46/EG) en heeft om die reden vergelijkbare bepalingen ten aanzien van de voorwaarden waaronder de gegevens in het watermerk mogen worden verwerkt.[156] Overtreding van de in deze wet opgenomen zorgvuldigheidsnormen vormen in beginsel een onrechtmatige handeling.[157] Hiermee is overigens niet gezegd dat de rechter hier ook expliciet aan toetst.[158]

---

[149] Verder wordt in de literatuur vooral gewezen op het beroepsgeheim, briefwisselingen, bestuursdocumenten, gerechtelijke akten of dossier en bemiddeling in familie zaken.
[150] Allemeersch & Schollen 2002, p. 56.
[151] Allemeersch & Schollen 2002, p. 56.
[152] Allemeersch en Schollen 2002, p. 55-57; Mougenot 2011, p. 242; Hendrickx 2006, p. 671; De Corte 2003, p. 809.
[153] Allemeersch & Ryelandt 2012, p. 166; Mougenot 2011, p. 242; Allemeersch en Schollen, 2002, p. 60.
[154] De Corte 2003, p. 802; Gutwirth, De Hert & Saelens 2007, p. 36. De Corte (2003, p. 803) wijst erop dat het om 'conceptuele redenen beter is de door de wet geregelde materies niet meer aan te duiden als een probleem van privacy, maar als autonome rechtsdomeinen, met hun eigen spelregels en voorwaarden. De term privacy kan dan best voorbehouden worden voor het restgebied, met andere woorden die domeinen waarop de regelgever zich nog niet heeft begeven'.
[155] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Daarnaast zou ook nog gedacht kunnen worden aan wetgeving ten aanzien van de watermerk service provider, zoals Wet op de bewakingsondernemingen, beveiligingsondernemingen, en de interne bewakingsdiensten 1990.
[156] Het is algemeen aanvaard dat de rechter bij discussies de WVP zoveel mogelijk Richtlijn-conform dient te interpreteren.
[157] Zie verder par. 5.3.2.1.
[158] Ook het Hof van Cassatie toetste hier bij het arrest van 2 maart 2005 niet expliciet aan. Cass. 2 maart 2005, P.04.1644.F, Arr.Cass. 2005, 506, JLMB 2005, 1086 m.nt. M. Beernaert, Journal Proc. 2005, nr. 499, 23, m.nt.

Op grond van de WVP dienen persoonsgegevens, evenals naar Nederlands recht, eerlijk en rechtmatig te worden verwerkt, voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen.[159] Deze gegevens mogen niet verder worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene, onverenigbaar is met die doeleinden.[160] Dat betekent onder meer dat persoonsgegevens op grond van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden dienen te worden verzameld en enkel verwerkt mogen worden als deze gelet op de doeleinden waarvoor ze worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.[161] Voor watermerken is het van belang dat iedere verwerking gebaseerd moet zijn op een zogenoemde verwerkingsgrondslag.[162]
Voor uitgebreide toelichting ten aanzien van de verwerkingsgrondslagen verwijs ik naar het Nederlandse recht in de voorgaande paragraaf. Evenals naar Nederlands recht is ook naar Belgisch privacyrecht, de ondubbelzinnige toestemming van de licentienemer de meest voor de handliggende grondslag voor de verwerking van persoonsgegevens.[163] Ook naar Belgisch recht is er weinig ruimte voor de stelling dat verwerking noodzakelijk is voor de uitvoering van een overeenkomst.[164] Ook naar Belgisch recht mag naar mijn mening de restbepaling van artikel 5 onder f WVP, waarin een grondslag kan worden gevonden wanneer de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor de verwerking of van de derde aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van deze wet, niet zwaarder wegen.[165]

Het recht op privacy is evenals naar Nederlands recht geen absoluut, maar is een functioneel recht waarbij in het kader van de rechtmatigheid een balans moet worden gezocht tussen verschillende rechten.[166] Wanneer de rechter tot de conclusie komt dat er sprake is van inbreuk op het privacyrecht van de licentienemer komt hij ook naar Belgisch recht toe aan de vraag of de schending gerechtvaardigd was. Dit criterium wordt enerzijds ingevuld door (nationale) beperkingen uit de WVP en anderzijds door de toetsing zoals deze is opgenomen in artikel 8 EVRM. In de praktijk zal deze snel gevonden kunnen worden in de toestemming van de licentienemer om zijn gegevens te verwerken.[167] Toestemming van de licentienemer

P. Toussaint; CR 2005/41, p. 258-263, m.nt. Van Eecke en B. Ooma (Chocolatier Manon). Zie voor commentaar op de privacyrechtelijke aspecten van die uitspraak o.m. Gurtwith, De Hert & Saelens 2007, p. 43.
[159] Art. 4. § 1 onder 1 en 2 WVP .
[160] Art. 4. § 1 onder 2 WVP.
[161] Art. 4. § 1 onder 3 WVP.
[162] Art. 5 WVP.
[163] Art. 5 onder a WVP.
[164] Art. 5 onder b WVP.
[165] De Koning kan, bij een in Ministerraad overlegd besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, nader bepalen in welke gevallen de onder f) bedoelde voorwaarde niet geacht wordt te zijn vervuld.
[166] Zie o.m. Cass. 7 oktober 1981, A.C. 1981-82, 1983; Cass. 27 februari 2001, RW 2001-2002, 1171; CBPL 2011, p. 9.
[167] Art. 1, §8 WVP.

heft ook het verbod van kennisnemen van elektronische communicatie op.[168] In de regel wordt aangenomen dat het voldoende is dit per overeenkomst te regelen of middels een scherm dat verschijnt alvorens de licentienemer tot aanschaf overgaat.[169]

In het licht van artikel 8 EVRM lijkt er weinig ruimte voor het toelaten van een rechtvaardigingsgrond voor het schenden van de privacy van de licentienemer wanneer er niet voldaan is aan de wettelijke verwerkingsgrondslagen. Zoals in de vorige paragraaf reeds is besproken laat het EHRM in de zaak Köpke/Duitsland zien dat de ernst van de fraude met zich mee kan brengen dat er sprake kan zijn van een rechtvaardigingsgrond wanneer er een concreet vermoeden bestaat dat een werknemer zich schuldig maakt aan strafbare feiten, welk vermoeden, anders dan met gebruikmaking van een verborgen camera niet zou kunnen worden bevestigd.[170] Het is tegen deze achtergrond dat het EHRM bereid is om onder bepaalde voorwaarden een rechtvaardigingsgrond aan te nemen. Hiervan is bij watermerken geen sprake. Hoewel de ernst van de inbreuk op het privacyrecht van de licentienemer in dit geval beperkt is gebleven tot het heimelijk verwerken van eenvoudige persoonsgegevens in een watermerk bestond er bij de rechthebbende ten tijde van het verwerken van de persoonsgegevens in het watermerk geen concreet vermoeden van onrechtmatig gedrag van een licentienemer. Daar komt bij dat de rechthebbende door toestemming te vragen gebruik had kunnen maken van een middel dat geen inbreuk maakt op de privacyrechten van de licentienemer. Bij watermerken is er geen reden voor de rechthebbende om in strijd te handelen met de voorwaarden die de WVP aan het verwerken van gegevens stelt. Wanneer hij dit nalaat handelt hij onrechtmatig en is een rechtvaardigingsgrond, evenals naar Nederlands recht, naar mijn mening niet snel meer denkbaar.

5.3.3 Strafrechtelijke onrechtmatigheid

In de situatie dat de rechthebbende het watermerk als bewijsmiddel aan de met opsporing belaste overheidsinstanties overhandigt en het OM dit watermerk als bewijs wil gebruiken doet zich ook in het strafrecht de vraag voor of de rechthebbende bij de verkrijging ervan in strijd gehandeld heeft met het privacyrecht. De beoordeling van de vraag of er sprake is van inbreuk op het privacyrecht van de licentienemer vindt plaats aan de hand van de hiervoor besproken civielrechtelijke criteria (par. 5.3.2.) en zal om die reden in de onderstaande subparagrafen slechts kort worden behandeld.

5.3.3.1 Nederland

[168] Artikel 124 j ° 125 van de wet betreffende de elektronische communicatie van 13 juni 2005; Cass. 1 oktober 2009, RG C.08.0064.N. Dit artikel vindt overigens slechts toepassing wanneer wij aannemen dat het watermerk niet persoonlijk voor de rechthebbende bestemd is. Ik zou zeggen dat in het kader van de uitvoering van de overeenkomst het watermerk ter controle bestemd is voor de rechthebbende, waardoor het artikel toepassing zou missen. Zie in dat kader ook de regeling ten aanzien van werknemers en werkgevers, CBPL 2011, p. 11.
[169] CBPL 2011, p. 10.
[170] EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, NJ 2011/566 m.nt. EJD (Köpke/Duitsland).

Het staat burgers in beginsel vrij om binnen de grenzen van het civiel- en strafrecht een bijdrage te leveren aan de strafrechtpleging.[171] Anders dan de met opsporing belaste overheidsinstanties zijn er geen nadere regels gesteld aan de wijze waarop zij bijdragen aan het vergaren van bewijs in strafzaken.[172] Niettemin kunnen burgers zich bij de opsporing van strafbare feiten ook zelf schuldig maken aan strafbare feiten, zoals diefstal.[173]

Strafrechtelijke vervolging van de inzet van strafbaar gestelde methoden, in het bijzonder bij de strafbepalingen van art. 139a t/m 139g Sr en art. 441b Sr, komt in de praktijk weinig voor.[174] Brinkhoff geeft daarvoor drie redenen.[175] Ten eerste kan het OM een strafrechtelijke vervolging onwenselijk achten, mede omdat een actievere burgerparticipatie bij criminaliteitsbestrijding wordt gestimuleerd. Ten tweede beperken diverse delicts-omschrijvingen het strafwaardige gedrag waardoor strafrechtelijke vervolging slechts beperkt mogelijk zal zijn. Ten derde komt strafrechtelijke vervolging mogelijk weinig voor omdat het bij de onderhavige strafbare feiten vaak gaat om een belangenafweging tussen twee of meer rechten waardoor het OM reeds bij de opportuniteitsafweging een afweging maakt die nadelig uitvalt voor de bescherming van de privacy van verdachte. Daarbij kan in het bijzonder worden gewezen op het feit dat de aanwezigheid van een rechtvaardigingsgrond aan een inbreuk het onrechtmatige karakter kan ontnemen. Of daarvan sprake is kan, zoals eerder reeds in het civiel recht is besproken, volgens de Hoge Raad slechts worden beoordeeld in het licht van de omstandigheden van het geval door de ernst van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer af te wegen tegen de belangen die met de inbreuk makende handelingen redelijkerwijs kunnen worden gediend.[176] In gevallen waarbij de privacy wordt geschonden ziet Kremer een rechtvaardigingsgrond in de situatie waarin de informatievergaring strekt ter verdediging van de rechtmatige belangen van de opsporende burger en/of ter openbaarmaking van onrechtmatig handelen van de onderzochte.[177] Een dergelijke belangenafweging doet zich ook voor in het civiel recht. Brinkhoff merkt onder verwijzing naar Kremer verder nog op dat er zich in de jurisprudentie ook een benadering voordoet waarin de Hoge Raad de persoonlijke levenssfeer zodanig inperkt dat aan een inbreuk op het privacyrecht niet meer wordt toegekomen.[178] Zo oordeelde de Hoge Raad in een strafzaak dat een verdachte die een telefoongesprek voert terwijl hij weet dat hij

[171] Zie o.m. Brinkhoff 2008, respectievelijk p. 71 en p. 68. Voor het civiele recht verwijs ik naar par. 5.3.2.1.
[172] Opsporingsambtenaren worden bijvoorbeeld beperkt door de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB), die mede gelet op de onschuldpresumptie en het recht op privacy bijzondere eisen stel aan de opsporing. Bij private opsporing kan gebruik worden gemaakt van particuliere beveiligingsorganisaties. Voor deze organisatie geldt naast het algemene recht, ook specifieke regelgeving in de vorm van de Wet particuliere beveiligingsorganisaties en recherchebureaus (WPBR).
[173] Brinkhoff 2008, p. 70; Buruma 2008, p. 49.
[174] Deze artikelen hebben volgens de MvT tot doel de persoonlijke levenssfeer doeltreffend te beschermen. Voor de beperkte vervolging zie o.m. Brinkhoff 2008, p. 71-72; Buruma 2008, p. 50; Brouwer 2008, p. 106.
[175] Brinkhoff 2008, p. 71-72.
[176] HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, NJ 1987/928 m.nt. E.A. Alkema (Grumbock/Van der Kaaij; Edamse bijstandsmoeder), ov. 4.4.; HR 31 mei 2002, ECLI:NL:HR:2002:AD9609, NJ 2003/589 m.nt. J.B.M. Vranken, ov. 3.5.2; meer recentelijk herhaalt in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.1
[177] Kremer 1999. In de jurisprudentie wordt met name de openbaar making zwaar aangerekend omdat in die gevallen het middel te zwaar is en hij naar de politie had moeten gaan. Maar die situatie doet zich hier niet voor.
[178] Brinkhoff 2008, p. 69. Kremer, ‘De grenzen van private opsporing’, Advocatenblad 2002, p. 6-11.

tegenover een politiefunctionaris zit, moet beseffen dat deze het gesprek kan horen. Van degene die onder de geschetste omstandigheden een telefoongesprek voert, kan immers niet worden gezegd dat hij voor wat betreft hetgeen hij uitspreekt, objectief gezien een redelijke verwachting heeft omtrent de bescherming van de persoonlijke levenssfeer.[179] Samenvattend dient de vraag naar de onrechtmatigheid van het watermerk als bewijsmiddel te worden beantwoord naar de criteria die gelden voor de beoordeling van de vraag of de rechthebbende inbreuk heeft gemaakt op de privacyrechten van de licentienemer. Zoals bij de bespreking van het civiel recht reeds aangegeven zie ik bij schending van de Wbp weinig ruimte voor het aannemen van een rechtvaardigingsgrond, nu de rechthebbende eenvoudig en met weinig kosten de voorzieningen kan treffen die recht doen aan de privacyrechten van de licentienemer.

Brinkhoff en Buruma pleiten er in Nederland voor om burgers (vaker) te vervolgen wanneer zij bijvoorbeeld grove inbreuk maken op de privacy.[180] De persoon die door deze handelingen verdacht geworden is moet volgens Buruma alleen dan worden vervolgd als daarmee een groot maatschappelijk belang is gediend.[181] Van een grove inbreuk op het privacyrecht van licentienemers lijkt bij watermerken, vanwege de beperkte inbreuk op dit recht, niet snel sprake te zijn. Het is, behoudens een snelle toename van het belang van privacy, ook niet snel denkbaar dat bij de vervolging een groot maatschappelijk belang is gediend.

5.3.3.2 België

In België strekt de regeling van onrechtmatigheid van bewijs er volgens Verstraeten wezenlijk toe de beklaagde een eerlijk proces te waarborgen[182] Om een dergelijk proces te waarborgen in het kader van het bewijs mag een materieel, formeel of algemeen rechtsbeginsel natuurlijk niet worden miskend.[183] Van oudsher wordt onrechtmatig bewijs in België gezien als bewijs dat is verkregen in strijd met het recht.[184] A-G Du Jardin heeft de term onrechtmatigheid van bewijs in een tweetal conclusies geplaatst in termen van waardigheid van het gerecht en het daaraan verbonden vereiste van loyaliteit.[185] Het gaat volgens hem daarbij om het vereiste van behoorlijkheid in de opsporing.[186] Deze behoorlijkheid ziet in het algemeen op het handelen van de van overheidswege ingestelde opsporingsinstanties. In de huidige situatie waarin

[179] HR 12 februari 2002 (strafkamer), ECLI:NL:HR:2002:AD5201, NJ 2002/330, ov. 3.4. Zie voor dezelfde overwegingen in het civiel recht par. 5.3.2.1.
[180] Buruma (2008, p. 59) in navolging van Brinkhoff (2008, p. 93).
[181] Buruma 2008, p. 54..
[182] Verstraeten 2012, p. 984. In dat licht spelen kan ook gewezen worden op artikel 6 EVRM en 14 IVBPR en de bijbehorende jurisprudentie.
[183] Verstraeten 2012, p. 985; Cass. 13 mei 1986, A.C. 1985-86, nr, 558; Cass. 23 maart 2004, AR. P. 04.0012. N.
[184] Cass. 12 maart 1923, Pas. 1923, I, 223; Cass 10 december 1923, Pas. 1924, 1, 66; De Decker & Verbruggen 2008, p. 68.
[185] Traest 2001, p. 65; Cass 13 mei 1986, A.C. 1985-86, nr. 558; Cass 4 januari 1994, A.C. 1994, I, nr. 1, RW 1994-1995, 187 m.n.t F. D'hont, Rec. Cass 1994, p. 72-75 m.nt. Ph Traest. In de Vlaamsetalige literatuur wordt dit laatste omschreven met de term loyauteit aan, wat overeenkomt met 'loyaliteit' in het Nederlands.
[186] Cass. 4 januari 1994, A.C. 1994, I, nr. 1, RW 1994-1995, 187 m.nt. F. D'hont, Rec. Cass 1994, p. 72-75 m.nt Ph Traest.

opsporingsinstanties voornamelijk optreden na tussenkomst van rechthebbenden ligt het plaatsen van watermerken door van overheidswege ingestelde opsporingsinstanties niet voor de hand.[187]

Voor het arrest van het Hof van Cassatie op 17 januari 1990 werd er geen onderscheid gemaakt tussen bewijs dat op een onrechtmatige wijze was verkregen door een van overheidswege ingestelde opsporingsinstantie of door een burger.[188] In dit arrest deed zich de situatie voor dat iemand een aantekenboekje met een schaduwboekhouding van de verdachte had gestolen met als doel hem hiermee later te chanteren. Na het wijzigen van zijn plannen heeft hij het betreffende boekje aan een ander gegeven die het vervolgens aan de politie heeft overhandigd. Het aantekenboekje kwam zodoende in de strafprocedure en werd als bewijs tegen de verdachte gebruikt.[189] Ongeveer een jaar later kwam een soortgelijke zaak aan de orde. In deze zaak had de echtgenote van de verdachte met wie hij in scheiding lag, gegevens gestolen en deze waren bij een huiszoeking naar aanleiding van de aangifte van de verdachte, bij diens vrouw in beslag genomen en in een zaak tegen hem gebruikt.[190]

Het Hof stelt in beide gevallen vast dat de met het onderzoek belaste personen en de aangever geen enkele onrechtmatige daad hebben gepleegd om in het bezit te komen van het betreffende bewijs. Bovendien ziet het Hof dat er geen verband bestaat tussen de diefstal en de overhandiging ervan aan de met het onderzoek belaste personen. In het laatste arrest merkt het Hof tevens op dat niets erop wijst dat de echtgenote de betreffende documenten in bezit hield om de vervolging van haar toenmalige echtgenoot op gang te brengen. In beide zaken maakt het Hof onderscheidt tussen de onrechtmatige wegneming en de verkrijging door de politie. Het Hof oordeelt dat uit het enkele feit dat de stukken onrechtmatig zijn weggenomen niet noodzakelijk volgt dat de overlegging daarvan ook onrechtmatig is. In het Nachtwakersarrest voegde het Hof hier aan toe dat de rechter een misdrijf niet bewezen mag verklaren wanneer het bewijs op een onrechtmatige wijze is verkregen hetzij door de overheid, hetzij door de aangever van het misdrijf.[191] Het Hof van Cassatie heeft in 1995 ook wel een onderscheid gemaakt tussen het bewijs van een overtreding en de aangifte daarvan.[192] De zaak betrof een in België gestart vooronderzoek op basis van gegevens die onrechtmatig waren verkregen door de Franse politie. In lijn met de eerdere jurisprudentie maakte het hof een onderscheid tussen de Franse rapportage en het Belgische bewijs. Dit is niet anders bij

[187] Par. 3.3.
[188] Cass. 17 januari 1990, A.C. 1989-90, nr. 130, Pas.1990, I, 588, RW 1990-1991, nr. 14, p. 463-464, m.nt. L.Huybrechts, RDPC 1990, 653 (Dutry); Cass, 29 oktober 1962, Pas. 1963, I, nr. 272; Zie ook Verstraeten 2012, p. 987; Traest 2001.
[189] Cass. 17 januari 1990, A.C. 1989-90, nr. 130, RW 1990-1991, nr. 14, p. 463-464, m.nt. L.Huybrechts, RDPC 1990, 653 (Dutry).
[190] Cass 17 april 1991, A.C. 1990-91, 834, Pas. 1991, I, 736, RW 1991-92, 403, noot A. Vandepas, RDPC 1992, p. 94-101 m.nt. C. De Valckeneer (Druart/Frejdun); Zie voor beide arresten ook Hutsebaut 1995, p. 209. Traest 2001, p. 64.
[191] Cass. 4 januari 1994, RW 1994-1995, 187 m.nt. F. D'hont, Rec. Cass 1994, p. 72-75 m.nt. Ph Traest.
[192] Zie ook Cass. 30 mei 1995, JLMB 1998, 488 m.nt. F. Kuty; Cass. 2 april 2008, AR P. 07.1744.F, JT 2008, 390, m.nt. F. kuyt; Cass. 18 mei 2011, AR P.10.2049.F; Traest 2005, p. 851; De Decker & Verbruggen 2008, p. 71; Verstraeten 2012, p. 988.

bijvoorbeeld een tap, waarbij onderscheid wordt gemaakt tussen enerzijds de beschikking tot afluisteren zelf en de uitvoering van de beschikking.[193]

Het Hof van Cassatie neemt thans als uitgangspunt dat uit het enkele feit dat bewijs bedrieglijk is verkregen niet noodzakelijk volgt dat het gebruik ervan in rechte onrechtmatig is.[194] Het gebruik van dat bewijs is slechts onrechtmatig indien de met het onderzoek belaste overheidsinstanties of de aangever zelf een onrechtmatigheid hebben begaan en er een verband bestaat tussen de door de derde gepleegde onrechtmatige daad en de overdracht van het bewijs. Dat wil zeggen dat de onrechtmatigheid werd begaan met de intentie het verkregen bewijs in een strafprocedure te gebruiken. Bewijs dat onrechtmatig is verkregen door bijvoorbeeld diefstal, maar door tussenkomst van een ander, aan de politie wordt overhandigd is in beginsel niet onrechtmatig.[195] In de literatuur wordt erop gewezen dat de situatie waarin een autoriteit in goed vertrouwen onrechtmatig verkregen bewijs kan gebruiken de procedure daarmee open staat voor het witwassen van onrechtmatig bewijs.[196] Het is duidelijk dat inbreuk op het privacyrecht bij bijvoorbeeld het verwerken van gegevens bij watermerken een onrechtmatige handeling is die is toe te schrijven aan de rechthebbende als aangever. Het zal ook duidelijk zijn dat hij de intentie had het watermerk als bewijs te gaan gebruiken in de (straf-)procedure. Hiermee zal het watermerk in beginsel als onrechtmatig kunnen worden gekwalificeerd. Van belang blijft wel dat vastgesteld moet worden dat er sprake is van inbreuk op het privacyrecht van de beklaagde. Daarvan zal niet snel sprake zijn omdat ook het Hof van Cassatie rekening houdt met de mate van intimiteit die in het gedrang is.[197] De mate van intimiteit is beperkt bij de verwerking van gegevens. Niet wordt uitgesloten dat het Hof van Cassatie bij watermerken niet snel zal aannemen dat er sprake is van inbreuk op het privacyrecht.

Het is niet duidelijk of het Hof van Cassatie ook na het in paragraaf 5.4.1.2 nader te bespreken Antigoon-arrest het onderscheid tussen onrechtmatigheden die begaan zijn door een derde of de overheid heeft willen handhaven.[198] Voor watermerken zal in beginsel gelden dat de overheidsinstantie totaal niet betrokken is bij het proces van watermerken (van aanbrengen tot interpretatie). Het verband tussen de door de derde gepleegde onrechtmatige daad en de overdracht van het bewijs kan meer problemen opleveren. Behoudens het feit dat de rechthebbende de resultaten van het onderzoek naar het watermerk via een ander rechtmatig aan de overheidsinstanties kan leveren, is het niet onbelangrijk dat het Hof van Cassatie er in

[193] Cass. 19 juni 2007, RABG 2008/7, m.nt .F. Van Volsem. Zie ook Huybrechts (1995, p. 52) die er al eerder op wees dat de nietigheid van de tapbeschikking alleen op de vormvoorschriften betrekking had.
[194] Verstraeten 2012, p. 987 en de hiervoor behandelde jurisprudentie.
[195] Dat is bijvoorbeeld het geval wanneer personeel dat toegang heeft tot bepaalde informatie deze aan de opsporingsinstanties overhandigt, omdat de verkrijging van die informatie enkel een contractuele inbreuk op de verhouding tussen de werkgever en werknemer inhoudt. Cass. 4 januari 1994, RW 1994-1995, 187 m.n.t F. D'hont, Rec. Cass 1994, p. 72-75 m.nt. Ph. Traest.
[196] Traest 2001, p. 71; De Decker & Verbruggen 2008, p. 71.
[197] Cass. 17 maart 2010, AR P. 09.1691.F, RW 2011-12, 1332, vgl. ook Cass. 5 oktober 2010, AR P.10.0703.N, T.Strafr. 2011, 66 m.nt. B. Meganck, RW 2011-12, p. 1338, m.nt. R. Saelens en P. De Hert.
[198] In haar eerste arrest van 14 oktober 2003 komt het onderscheid niet voor (mogelijk mede omdat die vraag niet voor lag) terwijl het Hof in het tweede arrest van 23 maart 2004 het onderscheid in stand laat.

het Nachtwakersarrest op wijst dat niets er in die zaak op wees dat de echtgenote de stukken onrechtmatig in bezit hield vanwege eventuele vervolging van de verdachte. Deze regels heeft het Hof later nogmaals herhaald.[199] De rechthebbende houdt, bij een vastgestelde schending van privacy, de stukken onrechtmatig in bezit vanwege eventuele vervolging van de verdachte.

Naar huidig Belgisch strafrecht zijn in het algemeen ten aanzien van onrechtmatig verkregen bewijs zowel in de literatuur als door het Hof van Cassatie drie soorten schendingen mogelijk: schending van (1) materiële en (2) formele beginselen en (3) de miskenning van algemene rechtsbeginselen.[200] In 2004 werd deze laatste categorie door het Hof van Cassatie in het zogenoemde Antigoon-arrest nader ingevuld door drie gronden: schending van het recht op privacy, miskenning van het recht op verdediging en het recht op menselijke waardigheid.[201] Het recht op privacy biedt ook in het strafrecht een bescherming tegen bezwarend gebruik van technieken waarvoor nog geen specifieke wettelijke basis bestaat.[202] Een miskenning van het recht kan onder meer gevonden worden in misleiding of het schenden van het zwijgrecht.[203] Het schenden van het recht op menselijke waardigheid moet volgens sommige auteurs niet als een aparte categorie worden opgevat omdat die situaties al in eerder genoemde domeinen kunnen worden geplaatst.[204] Deze situaties worden niet als limitatief beschouwd, nu het Hof van Cassatie bewijs dat in deze situaties is verkregen 'in principe' onrechtmatig verkregen acht. Hiermee lijkt er nog ruimte te zijn voor meer situaties. Hoewel in zaken waarbij het watermerk als bewijsmiddel een rol speelt alle situaties zich kunnen voordoen ligt met name de schending van privacy voor de hand wanneer het watermerk als bewijsmiddel geïsoleerd wordt benaderd. In de praktijk zou mogelijk ook nog sprake kunnen zijn van een poging tot misleiding door het voorleggen van bewijs, waarvan men weet dat het onbetrouwbaar is of ernstige twijfel daarbij heeft, teneinde de verdachte tot een bekentenis te brengen.

5.4 Gevolgen van onrechtmatig verkregen bewijs voor watermerken

In de voorgaande paragrafen is duidelijk geworden dat inbreuk op het privacyrecht van een licentienemer niet bij voorbaat kan worden uitgesloten, maar in de regel ook niet snel zal

[199] Cass. 4 januari 1994, A.C. 1994, nr. 1 RW 1994-1995, p. 185-188, m.nt. F. D'hont, Rec. Cass 1994, p. 72-75, m.nt. Ph. Traest; Cass. 9 december 1997, A.C. 1997, nr. 542, RW 1997-98, nr. 1441. Zie over deze arresten ook Hutsebaut 1995, p. 209.

[200] Cass. 13 mei 1986, A.C. 1985-1986, 558 (Belofte Belasting-ambtenaar). Bij materiële schendingen kan worden gedacht aan diefstal, afpersing of schending van het beroepsgeheim. Formele schendingen, zoals het niet in acht nemen van formele vereisten bij doorzoekingen (art. 138 Sv);

[201] Cass. 23 maart 2004, RABG 2004, p. 1061-1063, m.nt. Schuermans; RDPC 2005, 661 m.nt. C. De Valkeneer; en uitgebreid Verstraeten 2012, p. 1001.

[202] Zoals eerder bij cameratoezicht (inmiddels de wet aangenomen tot regeling van de plaatsing en het gebruik van bewakingscamera's (camerawet, BS 31 mei 2007, gewijzigd op 18december 2009). Zie o.m. De Decker & Verbruggen 2008, p. 70.

[203] Cass. 13 mei 1986, A.C. 1985-86, 558 (Belofte Belasting-ambtenaar); EHRM 5 november 2002 (Allen/VK).

[204] De Decker & Verbruggen 2008, p. 70.

voorkomen. Wanneer wij aannemen dat een watermerk in strijd met privacyregelgeving is verkregen rest de vraag welke gevolgen de rechter verbindt aan een dergelijke inbreuk.

In België is het leerstuk van het ongeoorloofd bewijs in burgerlijke zaken in verhouding met het strafrecht nauwelijks uitgewerkt waardoor er ook weinig lijn in de rechtspraak is.[205] Dit verschil laat zich mede verklaren doordat het Hof van Cassatie in 2003 voor de invulling van dit civielrechtelijke leerstuk aansluiting heeft gezocht bij de criteria die zij daarvoor in het strafrecht heeft geïntroduceerd in het Antigoon-arrest.[206] Vanwege de leesbaarheid, de invloed die het Belgische strafrecht heeft voor dit leerstuk op het Belgische civiel recht en de mogelijke invalshoeken die het Nederlandse strafrecht kan bieden voor het Nederlandse civiel recht wordt in deze paragraaf eerst het strafrecht behandeld en volgt daarna de behandeling van het civiel recht.

In het kader van het strafrecht staat de vraag centraal of watermerken die door de rechthebbende als private partij onrechtmatig zijn verkregen, door het OM wél als bewijs mogen worden gebruikt (par. 5.4.1). In het civiel recht is het de vraag of en onder welke omstandigheden het watermerk van het bewijs moet worden uitgesloten (par. 5.4.2).

5.4.1 Strafrechtelijke sancties op onrechtmatigheid

In paragraaf 5.3.2 is duidelijk geworden dat er onder omstandigheden sprake kan zijn van inbreuk op het privacyrecht van de licentienemer. De vraag die dan voorligt is of watermerken die door de rechthebbende als private partij onrechtmatig zijn verkregen, door het OM als bewijs mogen worden gebruikt in het kader van het leerstuk van het onrechtmatig verkregen bewijs.

5.4.1.1 Nederland

Het leerstuk van de onrechtmatige verkrijging van bewijsmateriaal betreft in het Nederlandse strafrecht grotendeels gecodificeerde rechtspraak en is wettelijk ingekaderd in artikel 359a WvSv.[207] In artikel 359a lid 1 WvSv zijn drie sancties opgenomen wanneer blijkt dat bij het voorbereidend onderzoek vormen zijn verzuimd die niet meer kunnen worden hersteld en de rechtsgevolgen hiervan niet uit de wet blijken.[208] De rechter heeft dan de keuze om (a) de hoogte van de straf in verhouding tot de ernst van het verzuim, te verlagen, wanneer het door het verzuim veroorzaakte nadeel langs deze weg kan worden gecompenseerd, (b) de resultaten

[205] Allemeersch & Van Orshoven 2011, p. 73; Laenens e.a. 2012, nr. 1349. p. 550.
[206] Cass. 10 maart 2008, S.07.0073.N, JLMB 2009, 580, m.nt. R. De Baerdemaeker, NjW 2010, 195, m.nt. K. Van Kildonck. Zie verder par. 5.4.1.2.
[207] HR 30 maart 2004, ECLI:NL:HR:2004:AM2533, NJ 2004, 376 m.nt. Buruma, herhaald in HR 4 januari 2011, ECLI:NL:HR:2011:BM6673, VA 2012/6, m.nt. M.L.C.C. de Bruijn-Lückers NJ 2012/145 m.nt. M.J. Borgers; Kst II 1994/95, 23705, nr. 3, p. 25-26. Zie voor de totstandkoming, achtergronden en kritische beschouwingen o.m. Embregts 2003, p. 99; Corstens 2014, p. 821; Nijboer 2011, p. 121 en de daar aangehaalde literatuur.
[208] Een onrechtmatigheid kan ook voorkomen tijdens het onderzoek ter terechtzitting en zal dan zoveel mogelijk tijdens het proces worden hersteld dan wel bij in appèl- of cassatie. Zie o.m. Corstens 2014. p. 822.

van het onderzoek die door het verzuim zijn verkregen niet te laten bijdragen aan het bewijs van het telastegelegde feit, (c) het OM niet ontvankelijk te verklaren wanneer door het verzuim geen sprake kan zijn van een behandeling van de zaak die aan de beginselen van een behoorlijke procesorde voldoet. De rechter dient hierbij rekening te houden met het belang dat het geschonden voorschrift dient, de ernst van het verzuim en het nadeel dat daardoor wordt veroorzaakt.[209] De wetgever heeft het herstel van het vormverzuim vooropgesteld en slechts sancties ter overweging gegeven wanneer herstel niet meer mogelijk is.[210] Als grondslag voor het strafrecht en tevens voor het uitsluiten van resultaten van onrechtmatige onderzoeks-activiteiten wordt in de literatuur met name het legaliteitsbeginsel genoemd.[211] Dit beginsel geeft uitdrukking aan de gedachte dat het optreden van de overheid dient te berusten op een wettelijke grondslag en geeft daarmee tevens invulling aan de gedachte van de rechtsstaat. Het beginsel geeft tevens een grens aan tot waar de overheid op rechtmatige wijze mag ingrijpen in de vrijheden en rechten van burgers.[212] Van de overheid en haar functionarissen mag zorgvuldig handelen worden verwacht. In dit kader wordt dan gesproken over de eisen van proportionaliteit en subsidiariteit, waarmee uitdrukking wordt gegeven aan de gedachte dat de door de overheid gekozen middelen in een redelijke verhouding staan tot het beoogde doel en het middel dat het minst ingrijpend is als eerste wordt gekozen.[213] In de rechtspraak en literatuur spreekt men bij het schenden van buitenwettelijke normen (onbehoorlijk overheidsoptreden) ook wel van het schenden van beginselen van een goede procesorde.[214] Artikel 359a Sv vindt geen toepassing wanneer derden op eigen initiatief en gezag bewijsverkrijgende handelingen hebben gepleegd die als onrechtmatig kunnen worden aangeduid.

De vraag die dan voorligt is of watermerken die door de rechthebbende als private partij onrechtmatig zijn verkregen, door het OM als bewijs mogen worden gebruikt. Wanneer wij vooropstellen dat het watermerk betrouwbaar is, dan rest de vraag of, en zo ja welke consequenties verbonden moeten worden aan het feit dat er bij de verkrijging van het bewijs in strijd is gehandeld met de privacyrechten van de licentienemer.

Het onrechtmatige handelen van de rechthebbende is bij watermerken gebaseerd op het schenden van het recht op privacy van de licentienemer op grond van artikel 8 EVRM en nationale privacywetgeving. De politie en het OM mogen als openbaar gezag op grond van het inmengingscriterium in onder meer artikel 8 lid 2 EVRM inbreuk maken op dit recht van privacy wanneer dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van onder meer de bescherming van de rechten en vrijheden van anderen. Dat

[209] Artikel 359a lid 2 WvSv.
[210] TK 1993/94, 23 705, nr. 3, p. 2. Artikel 359a Sv noemt in volgorde van zwaarte achtereenvolgens (a) strafvermindering, (b) uitsluiting, (c) niet-ontvankelijkheid van het OM (TK 1993/94, 23 705, nr. 3, p. 25).
[211] Zie o.m. Kremer 1999, p. 302; Embregts 2003, p. 103; Nijboer 2011, p. 31; Corstens 2014, p. 705, 817. Uitdrukking van deze gedachte kan in het recht worden teruggevonden in artikel 16 Gw en art. 7, lid 1 EVRM.
[212] Nijboer 2011, p. 32.
[213] Nijboer 2011, p. 122; in o.m. HR 12 december 1978, NJ 1979, 142; HR 6 april 1999, NJ 1999, 566 (Octopuszaak II) toetst de Hoge Raad beide beginselen aan toezeggingen aan getuigen.
[214] Nijboer 2011, p. 122; Cleiren 1989 (diss.).

brengt met zich mee dat wanneer zij, zonder dat de wet hierin voorziet, een rol hebben gespeeld bij de privacyschendende handelingen van de rechthebbende, aan deze schending het eerder besproken processueel gevolg van artikel 359a WvSV kan worden verbonden.
De Hoge Raad neemt als uitgangspunt dat wanneer natuurlijke of rechtspersonen voor of tijdens het voorbereidend onderzoek onrechtmatig hebben gehandeld het materiaal als bewijsmateriaal kan dienen, tenzij de overheid bij de onrechtmatige verkrijging verwijtbaar betrokken is of met het gebruik daarvan beginselen van een behoorlijke procesorde worden geschonden of de rechten van de verdediging veronachtzaamd,[215] bijvoorbeeld in het geval van foltering of wanneer het door derden aangedragen bewijs niet verifieerbaar is en de betrouwbaarheid van het materiaal niet kan worden beoordeeld.[216] Dat is ook het geval wanneer geheime diensten informatie aanleveren.[217] In dat geval zal ook de betrouwbaarheid van het bewijs een rol spelen. De sanctie van niet-ontvankelijkheid is in dit geval door de Hoge Raad tevens uitgesloten.[218] De Hoge Raad lijkt de fouten van derden niet aan het OM te willen toerekenen.[219]

Naar aanleiding van deze lijn van de Hoge Raad rest de vraag wanneer er sprake is van 'bemoeienis' of betrokkenheid van de overheid. De Hoge Raad is minder snel dan het EHRM geneigd bemoeienis in de vorm van advisering of technische ondersteuning aan te nemen.[220] De grens lijkt te liggen bij de vraag wie de uiteindelijke beslissing neemt om bijvoorbeeld een gesprek op te nemen. In navolging van het EHRM inzake M.M./Nederland betoogt ook Bleichrodt, anders dan de Hoge Raad dat het begrip bemoeienis van politie of OM niet te eng moet worden uitgelegd. Hiermee moet worden voorkomen dat de overheid zich aan haar

[215] HR 1 juni 1999, AA 49, 2000, p. 117-121 m. nt. YB; HR 11 april 1995, NJ 1995, 537, m.nt. Corstens (verkrijging door diefstal); HR 14 januari 2003, ECLI:NL:HR:2013:AE9038, NJ 2003, 288, .m.nt. YB; HR 18 maart 2003, ECLI:NL:HR:2003:AF4321, NJ 2003, 527 (foto's van particulier rechercherbureau); HR 8 november 2005, ECLI:NL:HR:2005:AU3292, NJ 2006/136; HR 14 november 2006, ECLI:NL:HR:2006:AX7471, NJ 2007, 179, m.n. YB (KB-Lux); HR 20 maart 2012, ECLI:NL:HR:2012:BV7501. Zie verder Corstens 2008, p. 710; Bleichrodt 2003 , p. 42-43. Dit lijkt in lijn met het EHRM: EHRM 23 november 1993, serie A, nr. 277-B (A/Frankrijk); EHRM 8 april 2003, NbSr 2003, 185 (M.M./Nederland) zo concluderen Minkenhof en Reijntjes 2009, p. 27. Zij merken tevens op dat het weinig verschil lijkt te maken of het materiaal gebruikt wordt in het kader van opsporing of bewijs. Zie voor het verschil tussen de HR en het EHRM ook Kuipers 2014 (diss.), p. 218. Zie verder ook Brinkhoff 2014 (diss.), p. 41.
[216] Zie o.m. Corstens 2014, p. 838.
[217] HR 5 september 2006 ECLI:NL:HR:2006:AV4122, NJ 2007/336, m.nt. Schaken; HR 15 november 2011, ECLI:NL:HR:2011:BP7544, NJ 2012/36 m.nt T.M. Schalken. Wanneer de verdediging zich beroept op strijd met een eerlijk proces vanwege de beperkte toetsing van de betrouwbaarheid van het bewijsmateriaal zal de rechter een grondig onderzoek moeten doen, waarbij de verdediging in de gelegenheid moet worden gesteld om de betrouwbaarheid van het materiaal aan te vechten. Bij een eventuele beperking van deze rechten dient de rechter naar compensatie te streven om langs andere wegen de betrouwbaarheid van het materiaal te onderzoeken. Met name de betrouwbaarheid van door geheime diensten aangeleverde informatie moet kritisch worden benaderd juist vanwege de beperkte controle die mogelijk is in het licht van de aard van deze diensten.
[218] Zie HR 1 juni 1999, AA 2000, p. 117, m.nt. Y. Buruma, ov. 3.2. Zie verder HR 14 november 2006, NJ 2007, 179 wordt in dit verband in algemene zin overwogen dat niet was gebleken dat 'overheidsdienaren' op enigerlei wijze bij de onrechtmatige verkrijging betrokken waren of deze hadden geïnitieerd of gefaciliteerd.
[219] Zie Bleichrodt 2010, p. 15, die deze gedachte aan vindt sluiten bij de verdeling van verantwoordelijkheden in het strafproces, waarbij in het algemeen niet past om het OM af te reken op fouten van derden. Dit mag evenals van andere auteurs niet leiden tot een situatie waarin de overheid zich onttrok aan haar publieke verantwoordelijkheid en de uitvoering van opsporingstaken de facto over laat aan particulieren.
[220] Vgl. HR 18 februari 1997, NJ 1997, 500 en de verwezen zaak EHRM 8 april 2003, NJCM-Bulletin 2003, p. 653-658 (M.M./Nederland).

verantwoordelijkheid onttrekt door het verzamelen van (onrechtmatig verkregen) bewijs aan haar burgers over te laten. Bleichrodt verstaat in navolging van de Hoge Raad onder bemoeienis het initiëren dan wel faciliteren van opsporingshandelingen door burgers.[221] Hij denkt daarbij aan situaties van substantiële advisering of met het oog op de opsporing het faciliteren van burgers. De grens lijkt daarbij te liggen bij de regie, wanneer de opsporingsautoriteiten deze overnemen is er sprake van bemoeienis. Ook in het geval waarbij sprake is van structurele samenwerking van politie of OM met degene die de informatie feitelijk heeft vergaard, zal eerder van bemoeienis kunnen worden gesproken. Temeer in die gevallen waarin afspraken zijn gemaakt dat de politie de uitkomst van particulier onderzoek afwacht voordat zij zelf in actie komt. Structureel wegkijken kan volgens Bleichrodt ook een vorm van bemoeienis opleveren.[222] Bleichrodt lijkt, zo constateren zowel Borgers als Kuiper, sneller verantwoordelijkheid aan te willen nemen dan de Hoge Raad.[223]

Kuiper is onder verwijzing naar Bleichrodt en Buruma van mening dat vanzelfsprekend voorkomen moet worden dat politie en OM gestimuleerd worden om zo min mogelijk verantwoordelijkheid te nemen voor wat derden in het kader van het onderzoek naar strafbare feiten doen.[224] Hij wijst erop dat de voor toerekening vereiste mate van betrokkenheid van politie of OM wel recht moet blijven doen aan het feitelijk bestaan van een situatie waarin zij verantwoordelijk is of verantwoordelijkheid zou moeten kunnen nemen. Kuiper heeft vooral moeite met het door Bleichrodt geformuleerde uitgangspunt wat betreft het toerekenen aan politie of OM bij ‘structureel wegkijken’ of het afwachten van de uitkomst van particulier onderzoek. Hij vreest dat dit een geheel nieuwe mer à boire aan verweren tot gevolg kan hebben, zonder dat de noodzaak van controle binnen het strafproces of het nut van toepassing van het de strafrechter ter beschikking staande reactiearsenaal evident is. De noodzaak van controle binnen het strafproces lijkt mij gelegen in de situatie dat voorkomen moet worden dat de politie of het OM de in het strafproces opgenomen waarborgen ter bescherming van de verdachte kunnen omzeilen door burgers het bewijs te laten verzamelen. Daarmee is tevens het nut gegeven van het reactiearsenaal. In veel gevallen zal strafvermindering uiteindelijk een redelijke sanctie zijn voor gevallen waarin er geen sprake is van grove schending van het recht. Wanneer in het particuliere onderzoek rechten van de verdachte zijn geschonden die niet raken aan zijn recht op een eerlijk proces in de zin van art. 6 EVRM, dan kan hij volgens Kuiper ook, of zelfs beter genoegdoening krijgen bij de civiele rechter.[225] Buruma stelde al eerder vast dat van strafrechtelijke vervolging in ieder geval weinig verwacht hoeft te worden.[226] Een veroordeling door de civiele rechter treft volgens Kuiper de onrechtmatig

[221] HR 14 november 2006, NJ 2007, 179, m.n. YB, ov. 3.5; Bleichrodt 2010, p. 17
[222] Bleichrodt 2010, p. 17.
[223] Borgers 2012, p. 408; Kuipers 2014 (diss.), p. 220.
[224] Bleichrodt 2010, p. 34 en vgl. Buruma 2011, p. 193 ‘de politie moet niet in de verleiding komen om onrechtmatige opsporingsmethoden te ‘outsourcen’ naar burgers’. Kuipers 2014 (diss.), p. 221.
[225] Kuiper 2014 (diss.), p. 221.
[226] Voor de beperkte vervolging in het strafrecht zie o.m. Brinkhoff 2008, p. 71-72; Buruma 2008, p. 50; Brouwer (2008, p. 106) concludeert dat erop de vraag of er behoefte is aan
fbaarstellingen om de meer extreme vormen van burgeropsporing aan banden te kunnen leggen, dat het probleem eerder ligt in de vervolgingspraktijk dan in het gebrek aan een wettelijk instrumentarium.

handelende particulier zelf en kan hem aanleiding geven zijn gedrag voortaan aan te passen. Tegen die achtergrond begrijpt Kuiper wel dat de Hoge Raad strikt vasthoudt aan haar eis dat overheidsdienaren op enigerlei wijze direct of indirect betrokken zijn bij het gewraakte optreden van de particulier of op enige andere wijze diens gedrag hebben geïnitieerd of gefaciliteerd.[227] Het belangrijkste lijkt mij dat, zoals Kuiper ook zelf aangeeft dat voor toerekening wel een mate van betrokkenheid van politie of OM moet zijn vereist waarin zij nog verantwoordelijkheid kan nemen. Het argument van Kuiper dat de verdachte terecht kan bij de civiele rechter mag in theorie waar zijn, maar zal er in de praktijk toe leiden dat de verdachte een kostbare procedure moet starten waarbij de uitkomst onzeker is. De kans dat de verdachte een dergelijke procedure zal starten lijkt mij klein. Het achterwege laten daarvan zal de onrechtmatig handelende particulier zeker geen aanleiding geven om zijn gedrag aan te passen. Zoals eerder gesteld, zal in veel gevallen strafvermindering uiteindelijk een redelijke sanctie zijn voor gevallen waarin er geen sprake is van grove schending van het recht. Het lijkt mij in geval van watermerken die als bewijsmiddel zijn ingezet om het auteursrecht te handhaven veel efficiënter wanneer de verrekening direct in het strafrecht plaatsvindt, omdat daarmee de rechthebbende aanleiding wordt gegeven om zijn gedrag aan te passen.

Gegeven dat er thans een aanwijzing van het OM ligt dat er eerst civielrechtelijk gehandhaafd moet worden is het handhaven van auteursrechten terecht geen prioriteit bij de politie. In die gevallen ligt het voor de hand, dat evenals in België het geval is, er tussen rechthebbende en de politie (structurele) afspraken worden gemaakt over het aanleveren van informatie en de wijze waarop dit dient te gebeuren. Zelfs wanneer er geen afspraken gemaakt zouden worden zal er na verloop van tijd een situatie ontstaan waarin de rechthebbende weet op welke wijze hij succesvol een dossier moet overhandigen. Het is daarbij van belang dat beide partijen in hun rol blijven.[228] Wanneer de politie of het OM streng toeziet op het materiaal dat men krijgt zal een rechthebbende niet snel geneigd zijn onrechtmatig te handelen. In de situatie waarin de rechthebbende en de politie afspraken hebben gemaakt over het aanleveren van informatie kan er, afhankelijk van de gemaakte afspraken mogelijk worden gesproken over het 'wegkijken' aan de zijde van de politie. Zonder dat er zoals Bleichrodt stelt, ook sprake is van een vorm van bemoeienis die tot uitsluiting van het bewijs kan leiden.[229] Buruma stemt in met de conclusie van Brinkhoff dat het bewijsmateriaal dat de burger door strafrechtelijk onrechtmatig te handelen op een haast professionele wijze heeft vergaard niet mag worden gebruikt. Buruma ziet daarbij een filterende rol weggelegd voor het OM. Met name in die gevallen waarin de gebruikte opsporingshandelingen niet in verhouding staan tot het opgespoorde delict.[230] De beperkte inbreuk op de privacy van de licentienemer alsmede het belang van de waarheidsvinding zal er bij watermerken aan bijdragen dat het in beginsel onrechtmatig verkregen bewijs niet snel zal worden uitgesloten.

[227] HR 10 april 2012, ECLI:NL:HR:2012:BU7636, NJ 2012/264.
[228] Zie o.m. de vele literatuur (o.m. Buruma 2010) die is verschenen naar aanleiding van de zogenoemde rechtelijke dwalingen als de Schiedamse parkmoord en Lucia de B.
[229] Bleichrodt 2010, p. 17.
[230] Buruma 2008, p. 54. Hij sluit dan ook niet dat bij ernstige delicten het OM wel gebruik wil kunnen maken van onrechtmatig verkregen bewijs door burgers.

Buruma komt tot de conclusie dat er door de rechter niet of nauwelijks consequenties verbonden worden aan onrechtmatige burgeropsporing, noch in de zin van vervolging noch in de zin van bewijsuitsluiting. Op grond van onder meer jurisprudentie van het Europese Hof voor de Rechten van de Mens komt hij tot de conclusie dat de rechter bij een sturende of faciliterende rol van politie of justitie tot bewijsuitsluiting kan besluiten. Hij ziet daar echter in de praktijk bijzonder weinig voorbeelden van en voegt daar aan toe dat 'rechtsvergelijking met de situatie in de VS of België suggereert dat het van een bijna onverantwoord idealisme getuigt, als men zou menen dat dit wat betreft het rechterlijk optreden anders zou kunnen'.[231] Dat is volgens Buruma hooguit anders 'voor zover de burgeropsporing wordt afgesloten met activiteiten die aan smaad of eigenrichting doen denken'.[232]

Afhankelijk van de ratio's (rechtsdoelen) die men hanteert vóór het uitsluiten van bewijs zal men tot de volgende conclusies komen.[233] Wanneer men als uitgangspunt neemt dat de overheid zelf moet laten zien dat het zich aan de regels moet houden (demonstratieargument) en het OM niet wist of redelijkerwijs kon vermoeden dat het bewijsmateriaal onrechtmatig is verkregen dan zal het materiaal moeten worden uitgesloten. Dat geldt ook wanneer men als uitgangspunt neemt dat de oude toestand (of het onrecht) zoveel mogelijk moet worden hersteld (reparatieargument). Het gevolg van de inbreuk op privacy dient dan hersteld te worden door het uitsluiten van het bewijs. Degene die gebruik maakt van een preventie of effectiviteitsargument ziet zich voor de keus gesteld waar hij het accent op moet leggen. Het preventieargument beoogt immers normconformgedrag. De overheid moet met bewijsuitsluiting worden afgehouden van onrechtmatige praktijken. Wanneer je gestolen bewijs uitsluit dan zit hier een preventieve werking in. Wanneer de overheid echter gesanctioneerd wordt wanneer zij bemoeienis heeft gehad met de onrechtmatige verkrijging dan doet de overheid er beter aan afstand te creëren tot de opsporende burger. Zowel ten aanzien van bewijs dat de burger heeft verzameld als bewijs dat verzameld is door geheime diensten geldt zoals Corstens terecht stelt in zijn annotatie 'passief blijven, doch met graagte accepteren, kan niet door de beugel'.[234] Brinkhoff merkt hierover op dat het in de eerste plaats aan de Officier van Justitie is om bij onrechtmatige verkregen informatie een afweging te maken tussen ernst van de onrechtmatigheid en het belang van de informatie voor de opsporing.[235] Dit maakt het mogelijk om het watermerk wel te gebruiken in het strafrechtelijke onderzoek en voor het toepassen van een dwangmiddel, maar niet om in te zetten als bewijsmiddel. Een onterechte toepassing kan echter wel tot strafprocessuele sanctionering leiden. Brinkhoff merkt op dat erop mag worden vertrouwd dat de Officier van

[231] Buruma 2008, p. 52. Er zijn geen aanwijzingen dat deze conclusive niet langer zou kunnen worden gedragen. Het is wel denkbaar dat de onthullingen van Snowden inzake de wijze waarop geheime diensten als derden informatie van grote groepen mensen verzamelen het standpunt over het uitsluiten van bewijs op termijn verandert.
[232] Buruma 2008, p. 59.
[233] Zie uitgebreid Embregts 2003, p. 104; Corstens 2014, p. 817.
[234] HR 11 april 1995, ECLI:NL:HR:1995:ZC9998, NJ 1995, 537 m.nt. Corstens, ov. 7.
[235] Brinkhoff 2014 (diss.), p. 41.

Justitie vanuit zijn professionaliteit de juiste keuze maakt. Het is uiteindelijk aan de rechter om hierover een definitief oordeel uit te spreken.
Een grove schending van privacy zal zich bij watermerken niet snel voordoen. Rechthebbenden die eenmaal worden aangesproken op deze schendingen zullen zelf of door tussenkomst van het OM of de rechter, snel tot een heroverweging komen omdat het watermerk als bewijsmiddel anders onbruikbaar wordt. In die zin zit er een mate van zelfregulering in.

5.4.1.2 België

Van oudsher wordt in België zowel het primaire als het secundaire (fruit of poisonous tree) onrechtmatig verkregen bewijs niet toelaatbaar geacht.[236] Hierbij werd geen onderscheid gemaakt tussen burgers en de politie.[237] Vanaf begin jaren negentig bracht het Hof van Cassatie op deze regels enige relativeringen aan, omdat de systematische uitsluiting van bewijs ook door burgers zal worden beschouwd als een tekortkoming in de plicht van de overheid om de maatschappij tegen misdaad te beschermen.[238] Wat het OM verkrijgt van derden mag zij gebruiken, voor zover bij de verkrijging daarvan geen grondrechtelijk beschermde waarborgen in het geding komen.[239]

Met de invoering van de kleine Franchimont in 1998 is de sanctionering van onrechtmatig bewijsmateriaal in België op twee wijzen gereguleerd.[240] In de eerste fase door de onderzoeksgerechten en in de tweede fase voor het vonnisgerecht.[241] De eerste fase door de onderzoeksgerechten wordt gekenmerkt door een wettelijk regime van zuivering van nietigheden. Sanctionering bij het vonnisgerecht is geregeld in de jurisprudentie en kent geen nadere wettelijke regeling.

Onrechtmatig verkregen bewijs dat bijdraagt aan de veroordeling van de verdachte is aan regels gebonden. Bewijs dat weliswaar onrechtmatig is verkregen, maar betrouwbaar en ontlastend is mag altijd worden gebruikt.[242] Op 14 oktober 2003 kwam het Hof van Cassatie

[236] Cass. 12 maart 1923, Pas. 1923, I, 223; Cass 10 december 1923, Pas. 1924, 1, 66; De Decker & Verbruggen 2008, p. 68; Demeersseman 2007, p. 202; Berneman 2004, p. 29; Verstraeten 2012, p. 1001.
[237] Zie o.m. Cass. 29 oktober 1962, RW 1963-64, p. 815. In dit arrest had de betrokkene het bewijs verkregen met het doel het later in een strafprocedure te gebruiken. Zie verder Corr. Brussel 18 april 1986, RW 1987-88, 60; zie ook Traest 2001, p. 63;Verstraeten 2005, p. 851; De Decker& Verbruggen 2008, p. 70.
[238] Zie Berneman 2004, p. 3.
[239] Zie o.m. EHRM 12 juli 1988, NJ 1988, 851 inzake Schenk; EHRM 27 juni 2001, NJ 2002, 102 (Rodriguez); EHRM 12 mei 2000, NJCM Bulletin, p. 1255, m.nt. E. Myjer ((Kahn/Verenigd Koninkrijk).
[240] Wet van 12 maart 1998 tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek, B.S. 2 april 1998. De ‘grote Franchimont’ waarin meer aandacht is voor de wijze waarop de rechter de overtreding van vormvoorschriften sanctioneert heeft het ondanks meerder pogingen tot op heden niet gehaald. Zie o.m. Verstraeten 2012, p. 1008.
[241] De eerste fase van onderzoeksgerechten vindt plaats voor het vonnisgerecht en vormt als het ware een filter tussen het onderzoek(sdossier) en de rechter. De raadkamer en in hoger beroep de kamer van inbeschuldigingstelling.
[242] Cass. 12 november 1997, RDPC 1998, 586; Cass 3 november 1999, TSR 2000, 255, m.nt. J. Meese; Verstraeten 2007, p. 870; De Decker & Verbruggen 2008, p. 72. De daaruit voortvloeiende problemen in relatie

in het zogenoemde Antigoon-arrest met een nieuwe koers, die inmiddels ook door het Arbitragehof en het Europese hof is goedgekeurd.[243] Het Hof van Cassatie stapte over van een systeem waar het uitsluiten van bewijs regel is naar een systeem waarbij de uitsluiting sterk beperkt is. Het Hof verplicht de feitenrechters om onrechtmatig verkregen bewijs in strafzaken uit te sluiten in drie situaties.[244] Anders gezegd uitsluiting van bewijs is nog slechts in drie gevallen toegestaan.[245]

De eerste situatie doet zich voor bij een op straffe van nietigheid voorgeschreven vorm.[246] De rechter beschikt daarmee niet langer over een appreciatiebevoegdheid en dient alleen de nietigheid vast te stellen.[247] Voor het gebruik van watermerken zijn deze bepalingen verder niet relevant omdat deze vormen zien op het optreden van de overheid en niet zoals in het geval van watermerken op het geval dat een derde deze vorm overtreedt.

Ten tweede kan het gaan om een situatie waarin de onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast.[248] Of daarvan sprake is blijft ter beoordeling van de rechter waardoor deze in beginsel niet tot cassatie kan leiden.[249] De betrouwbaarheid van het bewijs ziet op de verhouding tussen het bewijs en het te bewijzen feit. Een betrouwbaar bewijsstuk is in staat om de rechter ervan te overtuigen dat het te bewijzen feit heeft plaatsgevonden.[250] Het hof heeft met dit criterium de rechter expliciet de mogelijkheid gegeven het bewijs uit te sluiten buiten de bewijswaardering en beide categorieën om.[251] Het Hof van Cassatie lijkt normen die in de wet zijn vastgelegd om de intrinsieke waarde van het bewijsmateriaal te waarborgen (wettelijk bewijs), zoals bij DNA of ademanalysetesttoestellen voorlopig nog als een aparte categorie te zien die niet samenvalt met de Antigoon-toets.[252] De rechter mag bij schending van die bepalingen geen wettelijke bewijswaarde aan dat bewijs toekennen.

---

tot bewijs dat voor de ene verdachte ontlastend is en voor de ander belastend wordt verder buiten beschouwing gelaten.

[243] Cass. 14 oktober 2003, P.030762.N, *RABG* 2004, 333, m.nt. F. Schuermans (Antigoon); Cass. 23 maart 2004, P.04.0012.N, *RABG* 2004, 1061, m.nt. F. Schuermans'. Zie Schuermans (2010) in zijn noten onder EHRM 28 juli 2009, *RABG*, 2010/1 (Lee Davies/België) en GwH 22 december 2010, nr. 158/2010, RABG 2011, 563, m.nt. F. Schuermans; GwH 27 juli 2011, nr. 139/2011.

[244] De verplichting hiertoe is expliciet duidelijk geworden in Cass. 12 oktober 2005 P. 05.0119.F, TSR m.nt. Verbruggen.

[245] Historisch gaat het om het schenden van (i) materiële of (ii) formele wettelijke voorschriften of (iii) een algemeen rechtsbeginsel (Cass. 13 mei 1986, A.C. 1985-86, nr, 558) waarbij het Hof later (Cass. 23 maart 2004) deze laatste schending onderverdeeld in schending van een (1) recht op privacy en een miskenning van het (2) recht van verdediging en (3) het recht van op menselijke waardigheid. Zie o.m. Verstraeten 2012, p. 985.

[246] Zie voor een overzicht van de vormvoorwaarden voorgeschreven op straffe van nietigheid: Verstraeten 2012, p. 1007.

[247] Traest 2004, p. 137.

[248] Zie voor kritiek op dit criterium De Wolf 2004.

[249] Schuermans 2004a, p. 347; Traest 2004, p. 142; Verstraeten 2012, p. 1009.

[250] Traest 1992, p. 276.

[251] Verstraeten& De Decker 2005, p. 290.Hiermee is niet gezegd dat de rechter geen reden hoeft te geven waarom hij het bewijs onbetrouwbaarheid acht. Een verwijzing naar de onrechtmatigheid in relatie tot het bewijs lijkt voldoende.

[252] Cass. 25 mei 2005, JT 2005, 481, RDPC 2005, 1297; Cass. 26 november 2008, AR P.08.1293.F, RW 2010-11, 450. Het Hof casseerde in het eerste arrest de appelrechter die de antigoontoets had toegepast.

De derde en laatste situatie betreft het gebruik van bewijs dat in strijd is met het recht op een eerlijk proces.[253] De toelaatbaarheid van het bewijs dat de wet niet uitdrukkelijk uitsluit, moet worden beoordeeld in het licht van de artikelen 6 EVRM en 14 IVBPR, waarbij rekening moet worden gehouden met de elementen van de zaak in haar geheel genomen, inbegrepen de wijze waarop het bewijs verkregen werd en de omstandigheden waarin de onrechtmatigheid werd begaan.[254] Het Hof maakt ook duidelijk aan welke soort omstandigheden gedacht kan worden.[255]

Ten eerste het feit dat de overheid die met het onderzoek en de vervolging van misdrijven is belast de onrechtmatigheid opzettelijk heeft begaan (opzettelijkheid).[256] Het Hof heeft in zijn arrest van 12 oktober 2005 ook de aangever meegenomen in haar formulering waardoor niet mag worden uitgesloten dat het criterium van opzettelijkheid ook geldt voor de aangever en in dit geval de rechthebbende. Het is dan de vraag of er sprake is van een grove onachtzaamheid aan de kant van de rechthebbende. Afhankelijk van de omstandigheden van het geval kan ik mij voorstellen dat de rechter in beginsel het schenden van de voorlichtingsplicht in relatie tot het gemak waarmee de rechthebbende aan deze plicht kan voldoen, een grove onachtzaamheid acht. Het niet nemen van voldoende technische en organisatorische maatregelen is in abstracto veel lastiger te bepalen. Maar ook daar is een grove onachtzaamheid niet uit te sluiten.[257]

Ten tweede de situatie waarin de ernst van het misdrijf de begane onrechtmatigheid veruit overstijgt (proportionaliteit).[258] De vraag die dan voorligt is of het schenden van auteursrecht

[253] De feitenrechter kan het bewijs in deze nieuwe situatie dus ook toelaten wanneer het de vrucht van onrechtmatig overheidsoptreden betreft. Onduidelijk blijft of de rechter ook de (betrouwbare) vruchten van de nietige handelingen moet uitsluiten.

[254] Cass. 23 maart 2004, P.04.0012.N, RABG 2004, 1061, m.nt. F. Schuermans; Cass. 31 oktober 2006; Verstraeten 2012, p. 984. Inbreuk op een privacyrecht van de beklaagde geldt niet altijd als een schending van een eerlijk proces EHRM 12 mei 2000, (Khan/Verenigd Koninkrijk)

[255] Zie daarover o.m. de noten van F. Schuermans in zijn noot onder Corr. Gent 19 oktober 2005, T. Strafr. 2006, p. 42-43, nr. 13; Vandromme onder Cass. 12 oktober 2005, Vigiles 2006, p. 106-110; Van Volsem onder Cass. 19 juni 2007, RABG 2008/7, pp. 440-447.

[256] Het gaat hier niet alleen om doelbewuste maar ook om grove veronachtzaming van de belangen van de beklaagde (Cass. 23 september 2008, AR, P. 08.0519.N, TSR 2009, 151, m.nt. F. Schuermans; Cass. 26 januari 2011, AR P. 10.1321.F, RDPC 2012, 82, m.nt. D. Dillenbourg, TSR 2011, m.nt. F. Schuermans.

[257] Die vraag zal lastig blijven. Zo kan in Nederland worden gewezen op de zaak Diginotar waarbij duidelijk fouten zijn gemaakt maar erop papier ook voldoende waarborgen waren zoals een audit. Zie par. 6.4.2.

[258] Zo oordeelde correctionele rechtbank in Ieper dat het vaststellen van een verkeersovertreding door de politie in bijzijn van een camera-ploeg van VTM voor het programma ‘zwarte voet’, gezien de ernst van verkeersovertredingen het recht op privacy en een eerlijk proces had geschonden en niet kan worden gecompenseerd waardoor vrijspraak volgde. Corr. Rechtbank Ieper 26 mei 2005, AM 2005, 339, m.nt. J. Ceuleurs. Het cassatieberoep (Cass. 8 november 2005) werd verworpen vanwege het feit dat het voorrecht van de politie doelbewust is gedeeld met derden die van het begin op een actieve wijze bij initiële opsporing waren betrokken. Zie voor commentaar op deze uitspraak o.m. de noot onder dit arrest. Corr. rechtbank Dendermonde (29 maart 2006, T. Strafrecht 2007/2) laat in een vergelijkbare zaak weten dat de aanwezigheid van een derde niet noodzakelijkwijs leidt tot nietigheid van het bewijs. Ook dit blijft in cassatie (Cass. 21 november 2006, P. 060806.N) in stand omdat ‘de omstandigheden waarop hij dit oordeel grondt, zijn beslissing kunnen rechtvaardigen’ onder verwijzing van Cass., 8 nov. 2005, AR P.05.1106.N,nr 576. Vgl. ook Brussel 31 juli 2007 (niet gepubliceerd, ontleend aan Schuermans 2007, 12 september 2007, p. 8.) voor eenzelfde afweging ten aanzien van privacy inbreuk en het recht op een eerlijk proces in relatie tot de ernst van het feit (drugskoerier).

een ernstiger feit is dan het schenden van de privacyrechten van de beklaagde. Vooropgesteld kan worden dat de geschonden privacyrechten minimaal zijn in die zin dat er weinig sprake is van intimiteit.[259] Daar staat tegenover dat in literatuur het schenden van auteursrecht ook niet als een heel ernstig misdrijf wordt beschouwd.[260] Niettemin heeft de wetgever het OM de mogelijkheid willen geven om ambtshalve op te treden tegen auteursrechtinbreuk omdat de namaking in het auteursrecht als een verstoring of aantasting van de (economische) openbare orde wordt beschouwd. Een minimale inbreuk op het privacyrecht mag in deze afweging, mede in het licht van de waarheidsvinding er niet toe leiden dat het watermerk van bewijs zou moeten worden uitgesloten. De Corte stelt dat de rechter ook moet kijken naar het doel waarvoor het privacy(grond)recht werd toegekend.[261] Dat mag er volgens hem niet toe leiden dat iemand met een beroep op zijn privacyrechten ontsnapt aan de rechtsgevolgen van zijn handelen. Omdat iemand tijdens het plegen van een misdrijf niet bezig is met zijn zelfontplooiing en hierin ook geen beschermde ruimte kan worden gevonden die de maatschappij hem toe zou willen staan.[262] Hij ziet dan ook geen problemen wanneer een onrechtmatigheid aan het licht komt als gevolg van een schending van een privacyrecht. In de kern genomen laat De Corte anders gezegd de waarheidsvinding prevaleren boven het recht op privacy. Een redenering die ook het Hof van Cassatie in een zaak over ontslag na diefstal laat zien door te stellen dat de onregelmatigheid van deze onderzoeksdaad niet noodzakelijkerwijs de betrouwbaarheid van het bewijs aantast en derhalve de feitenrechter mag beslissen het bewijs te gebruiken zolang het recht op een eerlijk proces niet wordt aangetast.[263]

Ten derde de situatie dat het onrechtmatig bewijs slechts betrekking heeft op een materieel element van het misdrijf en ten vierde kan de vraag worden gesteld of de onregelmatigheid invloed heeft gehad op het doel van het geschonden voorschrift (doelbinding) en het louter formeel karakter van de onregelmatigheid (het vormvoorschrift). Het is uiteindelijk de rechter die, behoudens het marginale toetsingsrecht van het Hof van Cassatie, vrij oordeelt onder welke omstandigheden het gebruik van onrechtmatig verkregen bewijs in strijd is met het recht op een eerlijk proces.[264]

---

[259] Cass. 17 maart 2010, AR P. 09.1691.F, RW 2011-12, 1332, vgl. ook Cass. 5 oktober 2010, AR P.10.0703.N, T.Strafr. 2011, 66 m.nt. B. Meganck, RW 2011-12, p. 1338, m.nt. R. Saelens en P. De Hert.

[260] Zie Deene & Van der Perre 2005, p. 885.

[261] De Corte, p. 808

[262] De Corte ziet privacy dan ook als een ruimte voor zelfontplooiing. Zie daarover en commentaar daarop Gurtwith, De Hert & Saelens 2007, p. 38.

[263] Cass. 2 maart 2005, P.04.1644.F, Arr.Cass. 2005, 506, JLMB 2005, 1086 m.nt. M. Beernaert, Journal Proc. 2005, 499, 23, m.nt. P. Toussaint; CR 2005/41m p. 258-263, m.nt. Van Eecke en B. Ooma. (Chocolatier Manon). Zie voor commentaar op de privacyrechtelijke aspeten van die uitspraak o.m. Gurtwith, De Hert & Saelens 2007, p. 43. Zie in dezelfde lijn Cass. 5 oktober 2010, AR P.10.0703.N, T.Strafr. 2011, 66 m.nt. B. Meganck, RW 2011-12, p. 1338, m.nt. R. Saelens en P. De Hert waarin het Hof geen probleem ziet in het gebruik van camerabewijs ondanks dat de bewakingscamera slechts tot doel had handhaving van art. 135 Gem. wet. Zie ook Verstraeten 2012, p. 996.

[264] Zie o.m. Beernaert 2005, p. 1104. Annotatie onder Cass. 2 maart 2005; Verbruggen 2006, p. 29. Verstraeten & De Decker (2005, p. 296-297) hopen dat de cassatierechter dit marginale controlerecht substantieel invult vanwege haar rechtsvormende taak en het belang van behoorlijke opsporing in een rechtstaat. Dit lijkt tevergeefs zie o.m. Cass. 8 november 2005 en Cass. 21 november 2006, P. 060806.N; Verstraeten 2012, p. 1012.

De rechter kan thans op twee wijzen het watermerk toelaatbaar achten. Ten eerste kan hij ervoor kiezen om de verkrijging zelf niet als onrechtmatig te beschouwen. Hij kan er bijvoorbeeld voor kiezen om bij de vaststelling of er sprake is van inbreuk op het privacyrecht een afweging te maken waarin het belang van het auteursrecht prevaleert. Hierdoor is er weliswaar sprake van inbreuk op het privacyrecht maar wordt deze gerechtvaardigd waardoor er niet langer sprake is van een onrechtmatige handeling. Ten tweede kan de rechter de inbreuk op het privacyrecht vaststellen, maar later besluiten het bewijs niet uit te sluiten. Bijvoorbeeld door in het kader van eerlijk proces een afweging te maken tussen de ernst van de auteursrechtinbreuk in verhouding tot het privacyrecht.[265]

Het is aannemelijk dat de rechter het bewijs niet uitsluit omdat de eventuele schendingen van privacyrechten door de rechthebbende heeft plaatsgevonden en niet door het OM. Ook ondanks de meer algemene kritiek dat het niet uit moet maken wie de onrechtmatige daad heeft begaan voor de verkrijging van het bewijs werd het vanuit het oogpunt van de waarheidsvinding niet houdbaar geacht het bewijs uit te sluiten wanneer de overheid deloyaal of onrechtmatig gedrag kon worden verweten.[266]

Hoewel deze nieuwe koers in de praktijk minder vaak zal leiden tot uitsluiting van bewijs is het niet ondenkbaar.[267] Met name overwegingen ten aanzien van de betrouwbaarheid en de vraag of er sprake is van een eerlijk proces maken de uitsluiting nog mogelijk. Het is in de praktijk de feitenrechter, die ondanks de hoop die Verstraeten & De Decker uitspraken dat de cassatierechter zijn marginale controlerecht substantieel zou invullen vanwege het belang van behoorlijke opsporing in een rechtstaat, die bepaalt in hoeverre het bewijs wordt toegelaten.[268]

Met de Antigoon-leer is het nog steeds niet toegestaan om op onrechtmatige wijze bewijs te verzamelen, maar is de sanctionering zeer beperkt geworden. Niettemin kan ook worden geconcludeerd dat ook de onrechtmatigheid van door derden aan de overheid overhandigd bewijsmateriaal nog steeds kan worden witgewassen omdat het hof niet expliciet afstand heeft genomen van het eerder beschreven verschil tussen aangifte en bewijs. In die gevallen komt men niet meer toe aan de vraag of het bewijs moet worden uitgesloten.[269] Daarmee is de kans in de praktijk zeer klein geworden dat watermerken in België in een strafrechtelijke procedure worden uitgesloten als bewijs. De rechthebbende kan ervoor kiezen het bewijs wit te wassen door deze via een derde aan het OM te overhandigen. Daarnaast kan de rechter de handeling

[265] De afweging tussen de ernst van het misdrijf en de ernst van de inbreuk door de opspoorders moet hiermee worden beoordeeld binnen de grenzen van een eerlijk proces. Zie Verbruggen in zijn noot onder Cass. 12 oktober 2005.
[266] Zie Traest 1992, nrs. 672-673; Verstraeten 2012, p. 989. De overheid moet overigens de wil hebben hierover transparant te zijn. Het parket dat opzettelijk omstandigheden verbergt handelt in strijdt met het recht; Cass. 31 mei 2011, AR P. 10.2037.F, JT 2011, m.nt. M.-A. Beernaert, JLMB 2011, m.nt. A De Nauw.
[267] Cass. 16 november 2004, T. Strafr. 2005, 289-297; Verbruggen in zijn noot onder Cass 12 oktober 2005. Vgl. ook het EHRM bij de behandeling van zaken rondom fair trail (art. 6 EVRM).december 2005, 6.
[268] 2005, p. 296-297. Deze hoop lijkt tervergeefsgezien de huidige rechtspraak. Zie o.m. Cass. 8 november 2005 en Cass. 21 november 2006, P. 060806.N.
[269] Cass 23 maart 2004, (vnt 24); Cass. 19 oktober 2005, AR p.05.1287.F.

zelf niet als onrechtmatig kwalificeren en daardoor niet toekomen aan de vraag of het als bewijs moet worden uitgesloten en tot slot kan het watermerk toelaatbaar worden geacht door de toets uit de Antigoon-leer toe te passen.

In de literatuur is de nieuwe koers niet altijd positief ontvangen.[270] In het algemeen was er kritiek op het gebrek aan rechtszekerheid vanwege de niet nader ingevulde normen ten aanzien van de betrouwbaarheid en het recht op een eerlijk proces.[271] Tegenover deze kritiek staan ook auteurs die van mening zijn dat de waarheidsvinding het moet winnen van de terreur van de procedure mits met in achting neming van verantwoord samengestelde dossiers er betrouwbare bewijsgegevens worden gebruikt die een eerlijk proces niet in de weg staan.[272] In de praktijk is de vraag niet langer relevant of er sprake is van onrechtmatig bewijs. De vraag of het leidt tot uitsluiting is met deze nieuwe koers centraal komen te staan.[273] Daarbij lijkt vooral de vraag of het bewijs betrouwbaar is of niet van doorslaggevende betekenis.

De waarheidsvinding pleit in beginsel tegen het uitsluiten van bewijs dat weliswaar betrouwbaar is maar door een onrechtmatigheid niet zou kunnen worden gebruikt.[274] Daartegenover worden argumenten geplaatst die zien op de reparatie en demonstratie, alsmede de rechtstaatsgedachte dat de overheid zich ook aan de regels moet houden op straffe van sancties.[275] Traest plaatst ook privacy in de discussie over bewijsuitsluiting.[276]

5.4.2 Civielrechtelijke sancties op onrechtmatigheid

In de Nederlandse literatuur is men behoudens Kremer van oordeel dat onrechtmatig bewijs onder omstandigheden moet kunnen worden uitgesloten van het bewijs in een juridische procedure.[277] Verder gaat het in de literatuur in de kern om de afweging tussen de normschending en de waarheidsvinding, waarbij de omstandigheden van het geval of de wijze waarop het bewijsmateriaal is verkregen van invloed is op de toelaatbaarheid in de procedure.[278] Daarbij speelt in sommige omstandigheden tevens de vraag een rol of het gerechtvaardigd is dat een partij voordeel haalt uit bewijs dat in strijd met het recht is verkregen. De discussie in de literatuur spitst zich dan ook toe op de vraag onder welke

[270] Zie o.m. de noten van Kuty (2004) onder Cass. 14 oktober 2003; Traest 2004, p. 143; Beernaert (2005, p. 1109), Kuty 2005, Toussaint 2005 (allen onder Cass. 2 maart 2005); Hendrickx 2006, p. 685-687.
[271] Zie o.m. Schuermans 2004a, p. 354-7, 35; De Wolf 2004, p. 1238,; Van Eecke en OOMS onder Cass. 2 maart 2005; De Smet 2005, p. 255, en p. 258.
[272] De Smet 2005, p. 249; Schuermans 2004a, p. 354; Van Volsum 2008, p. 447.
[273] Verbruggen in zijn noot onder Cass 12 oktober 2005: Vindt het Spook van Antigoon rust? Franstalig 'schoonmoedersarrest' als slotluik van de nieuwe cassatierechtspraak over de uitsluiting van onrechtmatig bewijs?, p. 29; De Decker & Verbruggen 2008, p. 66.
[274] Zie ook Traest 2001, p. 66.
[275] Zie o.m. Traest 2001, p. 66; Corstens 2014, p. 817; Embregts 2003, p. 104.
[276] Zie ook Traest 2001, p. 66; Berneman 2004.
[277] Zie o.m. De Bock 2011 (diss.), par. 4.8; Asser 2013, p. 155. Kremer 1999 (diss.) zoekt in hoofdstuk acht van zijn proefschrift de sanctie van onrechtmatig verkregen bewijs in schadevergoeding.
[278] Zie ook A-G Asser ov. 4.11 voor HR 16 oktober 1987, NJ 1988, 850, m.nt. EAA (Driessen/Van Gelder).

omstandigheden onrechtmatig bewijs moet worden uitgesloten in een procedure.[279] In de volgende paragraaf wordt gekeken op welke wijze in de Nederlandse rechtspraak wordt omgegaan met het sanctioneren van onrechtmatige verkregen bewijs (par. 5.4.2.1).

In België was tot 2003 het algemene uitgangspunt dat onrechtmatig verkregen bewijs in beginsel niet in rechte kan worden aangewend en daarom was uitgesloten van bewijs.[280] In 2003 aanvaardde het Hof van Cassatie in het Antigoon-arrest het gebruik van onrechtmatig verkregen bewijs in strafzaken en in 2008 in civiele zaken onder een aantal voorwaarden. Met name in het Belgische civiel bewijsrecht is er vanwege deze recente ontwikkelingen beperkte aandacht voor het sanctioneren van onrechtmatig verkregen bewijs (par. 5.4.2.2).

5.4.2.1 Nederland

In de vorige paragraaf is duidelijk geworden dat naar Nederlands recht onder omstandigheden het verwerken van gegevens in het watermerk onrechtmatig kan zijn en er derhalve toe kan leiden dat het watermerk als onrechtmatig verkregen bewijs kan worden gekwalificeerd. De vraag die zich dan bij het leerstuk van het onrechtmatig verkregen bewijs voordoet is of het watermerk ook van het bewijs moet worden uitgesloten.[281]

Het dilemma dat zich voordoet bij het leerstuk van het onrechtmatig verkregen bewijs is dat een partij bewijs dat jegens hem onrechtmatig is verkregen buiten beschouwing van de rechter wil laten, terwijl de waarheidsvinding met zich meebrengt dat zoveel mogelijk betrouwbare informatie beschikbaar komt, zodat er recht kan worden gedaan op een juiste feitelijke grondslag die overeen komt met de werkelijkheid.[282]

De discussie in de literatuur gaat vooral over de vraag onder welke omstandigheden onrechtmatig verkregen bewijs in een procedure zou moeten worden uitgesloten.[283] Kremer is van mening dat omwille van de waarheidsvinding relevant en betrouwbaar bewijs altijd moet worden toegelaten en dat een sanctie voor het gebruik of de verkrijging van dat bewijs gevonden kan worden in een schadevergoeding.[284]

---

[279] Zie daarvoor de dissertaties van Kremer 1999 (diss.) en Embregts 2003 (diss.).
[280] Cass. 12 maart 1923, Pas.1923, I, 323; Cass. 18 april, 1985, A.C. 1984-85, 1102; Allemeersch & Schollen, p. 50. Niettemin was er verdeeldheid in de lagere rechtspraak. Waar een deel van de rechtspraak al wel rekening hield met omstandigheden van de zaak. Zie ook Allemeersch & Van Orshoven 2011, p. 76.
[281] Zie o.m. Embregts (diss. 2003), p. 237; De Bock (diss.) 2011, p. 178; Asser 2013, nr 145, p. 157. HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.3
[282] Zie ook Asser 2013, nr. 143, p. 156.
[283] Zie Embregts 2003 (diss.), p. 237; De Bock (diss.) 2011, p. 178; Asser 2013, nr 145, p. 157. Kremer 1999 (diss.), p. 301.
[284] Kremer 1999 (diss.), p. 301. Kremer (p. 304) lijkt uitsluiting van het bewijs wel denkbaar te achten in het geval de onrechtmatigheid van de bewijsverkrijging samenvalt met een aantasting van echte processuele rechten. Maar zo constateert Kremer direct, ‘een dergelijke samenval is echter bepaald geen regel‘. Daarna lijkt hij echter er geen rol meer te zien voor bewijsuitsluiting en de schadevergoeding te prevaleren boven bewijsuitsluiting.

De vraag of informatie die via het watermerk op een onrechtmatige wijze is verkregen van het bewijs moet worden uitgesloten moet bij gebrek aan wettelijke criteria beoordeeld worden aan de hand van in de jurisprudentie en literatuur.

De Hoge Raad maakt in zijn arrest van 18 april 2014 (Achmea/Rijnberg) duidelijk welke invulling zij geeft aan het leerstuk van het onrechtmatig verkregen bewijs. De Hoge Raad neemt artikel 152 Rv als uitgangpunt door te stellen dat bewijs door alle middelen kan worden geleverd en dat de waardering van het bewijs aan het oordeel van de rechter is overgelaten, tenzij de wet anders bepaalt.[285] In een civiele procedure is er volgens de Hoge Raad in ieder geval geen algemene regel dat de rechter op onrechtmatig verkregen bewijs geen acht mag slaan. Ten aanzien van het eerder geschetste dilemma stelt de Hoge Raad dat het algemene maatschappelijke belang dat de waarheid in rechte aan het licht komt, alsmede het belang dat partijen erbij hebben hun stellingen in rechte aannemelijk te kunnen maken, in beginsel zwaarder wegen dan het belang van uitsluiting van bewijs. Het uitsluiten van het bewijs is volgens de Hoge Raad dan ook slechts gerechtvaardigd, indien sprake is van bijkomende omstandigheden.[286]

De invulling die de Hoge Raad in dit arrest geeft aan het leerstuk van de onrechtmatige daad ligt in de lijn van zijn eerdere arresten.[287] Dat de waarheidsvinding in beginsel van een groter belang is dan het uitsluiten van het bewijs werd al eerder duidelijk in het arrest Overbeek toen de Hoge Raad overwoog dat in het kader van het leveren van bewijs het belang van privacy moet wijken voor het belang van de waarheidsvinding.[288] Een verwijzing naar het arrest Overbeek laat de Hoge Raad in zijn arrest Achmea/Rijnberg echter achterwege.

Ook de overweging dat het uitsluiten van het bewijs slechts gerechtvaardigd, indien sprake is van bijkomende omstandigheden past in de lijn van zijn eerdere arresten. Dat de Hoge Raad het uitsluiten van het bewijs slechts gerechtvaardigd acht, indien sprake is van bijkomende omstandigheden past in de lijn dat de Hoge Raad al jaren terughoudend is ten aanzien van het uitsluiten van het bewijs.[289] Bij het beoordelen van daartoe voorgestelde middelen komt de Hoge Raad bijna altijd tot het oordeel dat het bewijs niet onrechtmatig is verkregen en komt

[285] Zie art. 152 Rv en HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.2.3.
[286] De Hoge Raad verwijst in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.3 voor dit standpunt onder meer naar HR 7 februari 1992, ECLI:NL:HR:1992:ZC0500, NJ 1993/78, ov. 3.5.2 (Slempkes/Nool) en HR 12 februari 1993, ECLI:NL:HR:1993:AJ8237, NJ 1993/599 m.nt. H.J. Snijders & E.A. Alkema (Spijkenisse). Ten aanzien van dit laatste arrest verwijst de Hoge Raad (ov. 5.2.3) naar het verkeerde ECLI-nr (ZC0860 i.p.v. AJ8237). Herhaald in HR 11 juli 2014, ECLI:NL:HR:2014:1632.
[287] Vgl. A-G Wissink in zijn conclusie voor HR 11 juli 2014, ECLI:NL:HR:2014:1632. Hij verwijst daar bij naar de conclusie van de plv. procureur-generaal voor HR 18 april 2014, ECLI:NL:PHR:2014:942, ov. 18; Asser 2013, nr. 147, p. 159; De Bock 2011 (diss.), p. 179; Embregts 2003 (diss.), p. 245. Vgl. voorts de opvattingen van Kremer 1999 (diss.), p. 296 en 304-306.
[288] HR 11 september 1998, ECLI:NL:HR:1998:ZC2701, NJ 1999/664 m.nt. M.M. Mendel (Overbeek), ov. 3.3: 'voorzover de overlegging van het proces-verbaal al als een inbreuk op hun privacy is te beschouwen, het belang van K. en J. bij bescherming van hun privacy moet wijken voor het belang van Oost Nederland dat in de onderhavige procedure de waarheid van de door haar gestelde feiten komt vast te staan'.
[289] De Bock (diss.) 2011, p. 180 constateerde al eerder dat de Hoge Raad zelden een beroep op uitsluiting van het bewijs honoreert. Vgl. ook Asser, p.159.

dan niet meer toe aan de vraag of het bewijs moet worden uitgesloten.[290] Daarbij speelt in het bijzonder dat de Hoge Raad bij inbreuk op privacyrechten al bij de beoordeling van de vraag of het bewijs in strijd met de bescherming van de persoonlijke levenssfeer is verkregen, de omstandigheden van het geval een rol laat spelen. Dit heeft tot gevolg dat in de rechtspraak in veel gevallen niet meer wordt toegekomen aan de vraag of bewijs moet worden uitgesloten.[291] Het komt ook voor dat de Hoge Raad het antwoord op de vraag of er sprake is van onrechtmatig verkregen bewijs in het midden laat, vanuit de gedachte dat onrechtmatig verkregen bewijs in beginsel bruikbaar is in een civiele procedure.[292] In de meeste zaken komt de Hoge Raad tot de conclusie dat het bewijs niet onrechtmatig is verkregen. Asser komt ten aanzien van de gehele rechtspraak tot een vergelijkbare conclusie wanneer hij stelt dat de meeste rechtspraak de vraag betreft naar de onrechtmatigheid van de verkrijging en niet de vraag of de informatie moet worden uitgesloten.[293]

Evenals de rest van de literatuur is ook de Hoge Raad van oordeel dat uitsluiting van het bewijs enkel gerechtvaardigd is wanneer er sprake is van bijkomende omstandigheden.[294] Wanneer er sprake is van dergelijke bijkomende omstandigheden is uit de rechtspraak van de Hoge Raad lastig op te maken omdat de Hoge Raad tot het arrest Achmea/Rijnberg niet verder is gekomen dan de constatering dat voor uitsluiting van het bewijs bijkomende omstandigheden vereist zijn.[295]

In het arrest Achmea/Rijnberg lag de zaak voor of een verzekeraar die in strijd handelde met de door het Verbond van Verzekeraars opgestelde Gedragscode, door een persoonlijk onderzoek in te stellen naar een verzekerde, de resultaten van dat onderzoek voor het bewijs mocht gebruiken.[296] De Hoge Raad bevestigt in dit arrest kort gezegd het oordeel van het hof dat wanneer het Verbond van Verzekeraars met deze gedragscode invulling heeft gegeven aan een belangenafweging die nodig is om te kunnen bepalen of er sprake is van een

[290] Zie ook De Bock (diss.) 2011, p. 180. Asser 2013, nr. 146, p. 157. De Bock (diss.) 2011, p. 180 wijst voor een uitzondering naar HR 30 november 2001, ECLI:NL:HR:2001:AD4000 NJ 2002, 462 m.nt. JdB. Ik deel die mening niet. De Hoge Raad laat m.i. in het midden of er sprake is van schending van het recht wanneer zij stelt (ov. 3.2.5): 'SJG heeft zich niet op enige wettelijke bepaling beroepen op grond waarvan of krachtens welke zij de bevoegdheid heeft de vader te dwingen mee te werken aan video-opnamen, die een inbreuk zouden kunnen betekenen op zijn in art. 10 Gr.w. beschermde recht op eerbiediging van zijn persoonlijke levenssfeer'. Een uitzondering kan m.i. wel worden gevonden in HR 11 september 1998, ECLI:NL:HR:1998:ZC2701, NJ 1999/664 m.nt. M.M. Mendel (Overbeek), ov. 3.3 en inmiddels in HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.2.2.

[291] Zie ook HR 11 juli 2014, ECLI:NL:HR:2014:1632, gewezen na HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg).

[292] Zie o.m. HR 11 september 1998, ECLI:NL:HR:1998:ZC2701, NJ 1999/664 m.nt. M.M. Mendel (Overbeek), ov. 3.3. Zie in de lagere rechtspraak, o.m. Rb. Rotterdam 6 augustus 2008, ECLI:NL:RBROT:2008:BD9713, ov. 5.4.

[293] Asser 2013, nr. 146, p. 157.

[294] De Hoge Raad verwijst in HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.3 voor dit standpunt onder meer naar HR 7 februari 1992, ECLI:NL:HR:1992:ZC0500, NJ 1993/78, ov. 3.5.2 (Slempkes/Nool) en HR 12 februari 1993, ECLI:NL:HR:1993:AJ8237, NJ 1993/599 m.nt. H.J. Snijders & E.A. Alkema (Spijkenisse), ov. 3.3.2. Ten aanzien van dit laatste arrest verwijst de Hoge Raad (ov. 5.2.3) naar het verkeerde ECLI-nr (ZC0860 i.p.v. AJ8237).

[295] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg).

[296] Idem.

onrechtmatige inbreuk op de persoonlijke levenssfeer van de verzekerde, er gelet op de inhoud en opzet van de Gedragscode tot uitgangspunt kan worden genomen dat indien een verzekeraar in strijd met de code handelt, sprake is van onrechtmatig verkregen bewijs.[297]

In deze zaak komen zowel het hof als de Hoge Raad vervolgens toe aan de vraag of onrechtmatig verkregen bewijs in een procedure kan worden meegewogen en welke belangen daartoe moeten worden afgewogen.[298] Bij deze afweging gaat het volgens het hof enerzijds om het belang van waarheidsvinding en anderzijds om het belang van een rechtens verantwoorde bewijsgaring die er mede uit zou bestaan dat een rechtsinbreuk niet gehonoreerd mag worden. Volgens het hof is daarbij in de kern aan de orde of het gerechtvaardigd is dat een procespartij die op onrechtmatige wijze bewijs heeft verkregen, wordt beloond door dit bewijs in de procedure tot haar voordeel te betrekken. Bij dat oordeel betrekt het hof opnieuw dat het hier gaat om schending van een door het Verbond van Verzekeraars voor haar leden opgestelde gedragscode, die een toetsingskader beoogt te bieden voor het instellen van het persoonlijk onderzoek. Het strookt volgens het hof, ook in een geval waarin de ernst van de inbreuk op de persoonlijke levenssfeer gering is, niet met het doel van deze vorm van zelfregulering om een verzekeraar die deze gedragscode schendt te belonen door het onrechtmatig door haar verkregen bewijs tot haar voordeel te laten strekken. Bij de beoordeling van de toelaatbaarheid van het bewijs acht het hof voorts van belang dat de verzekeraar onvoldoende alternatieve wijzen van informatieverzameling heeft benut om te bezien of haar gestelde vermoeden van fraude ontkracht kon worden en tevens niet gezegd kan worden dat de verzekerde door zijn opstelling de onoorbare wijze van bewijsgaring heeft uitgelokt of in de hand heeft gewerkt. Het hof komt dan ook tot het oordeel dat het de resultaten van het persoonlijk onderzoek bij de verdere beoordeling buiten beschouwing zal laten. Het hof ziet in deze zaak kennelijk een bijkomende omstandigheid in de overweging dat iemand die het recht schendt niet beloond mag worden door bewijs te mogen gebruiken dat door haar op een onrechtmatige wijze is verkregen.

In cassatie wordt betoogd dat de vaststelling dat met het onderzoek vergaarde bewijs onrechtmatig is verkregen, niet zonder meer meebrengt dat dit bewijs buiten beschouwing moet blijven bij de verdere beoordeling van het geschil.[299] Volgens de Hoge Raad is dit onderdeel tevergeefs voorgesteld, omdat het hof zijn beslissing om de resultaten van het persoonlijk onderzoek buiten beschouwing te laten niet gegrond heeft op de enkele omstandigheid dat Interpolis niet gerechtigd was tot het doen uitvoeren van dat onderzoek.[300] Het hof heeft volgens de Hoge Raad mede het doel van de Gedragscode in aanmerking genomen, waarmee niet strookt dat in de omstandigheden van dit geval in strijd daarmee verkregen bewijsmateriaal toch door een verzekeraar kan worden gebruikt. De hier door de Hoge Raad bedoelde omstandigheden van dit geval slaan terug op omstandigheden dat de

[297] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.2.1.
[298] Hof ‘s-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465, ov. 35 en 36; HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.3.2 (Achmea/Rijnberg).
[299] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.4.1.
[300] HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), ov. 5.4.2.

verzekeraar bij haar beslissing onvoldoende acht heeft geslagen op het subsidiariteitsbeginsel doordat de verzekeraar niet in redelijkheid heeft kunnen vermoeden dat de verzekerde haar bij de uitvoering van de schadebehandeling grondig en/of structureel heeft misleid en er ook geen sprake was een structureel gebrek aan medewerking van de verzekerde om de benodigde feiten te verzamelen.[301] De Hoge Raad sluit af met de overweging dat voor zover het onderdeel het hof verwijt noch de beperkte ernst van de inbreuk, noch de ernst van de gestelde fraude in zijn afweging te hebben betrokken, het onderdeel terecht feitelijke grondslag mist. De Hoge Raad laat hiermee het oordeel van het hof in stand dat het onrechtmatig verkregen bewijs in dit geval van het bewijs mocht worden uitgesloten. Het is echter onduidelijk welke bijkomende omstandigheden de Hoge Raad in deze zaak van belang acht om het onrechtmatig verkregen bewijs buiten beschouwing te laten.[302]

Het arrest roept de vraag op of omstandigheden die een rol spelen bij de vraag of er sprake is van een rechtvaardigingsgrond die het onrechtmatige karakter kan ontnemen dezelfde omstandigheden zijn die een rol spelen bij de vraag of het onrechtmatig verkregen bewijs van het bewijs moet worden uitgesloten. Krans verwoordt het mooi wanneer hij schrijft dat ‘de omstandigheden en elementen figureren in de rechtsoverwegingen’. De Hoge Raad beperkt zich bij het antwoorden van het middel tot het voorgestelde onderdeel waardoor verder niet duidelijk wordt welke omstandigheden nu precies in welke context een rol spelen bij het beantwoorden van de vraag welke bijkomende omstandigheden nu van belang zijn om het uitsluiten van het bewijs te rechtvaardigen.

De Hoge Raad maakt in deze zaak gebruik van twee omstandigheden die volgens hem tot het oordeel leiden dat het in dit geval gerechtvaardigd is om onrechtmatig verkregen bewijs van het bewijs uit te sluiten. Ten eerste de omstandigheid dat het doel van de Gedragscode niet strookt met het idee dat in strijd daarmee verkregen bewijsmateriaal toch door een verzekeraar kan worden gebruikt. De Hoge Raad lijkt hiermee te gaan met het oordeel van het hof dat ook in een geval waarin de ernst van de inbreuk op de persoonlijke levenssfeer gering is, het niet met het doel van deze vorm van zelfregulering strookt om een verzekeraar die deze gedragscode schendt te belonen door het onrechtmatig door haar verkregen bewijs tot haar voordeel te laten strekken. Krans is van mening dat wanneer er sprake is van een beperkte inbreuk op de persoonlijke levenssfeer het uitsluiten van bewijs niet voor de hand ligt, maar dat de Hoge Raad in dit arrest omstandigheden heeft aangetroffen die kennelijk meer gewicht krijgen.[303] Hij stelt dat de overwegingen van de Hoge Raad doen vermoeden dat het vooral

[301] Krans (in zijn noot onder dit arrest NJ 2015/20) merkt hierover op dat de Hoge Raad in zijn eigen overwegingen omtrent het uitsluiten van bewijs (ov. 5.4.2) ook naar de feiten verwijst in zijn eigen samenvatting (ov 3.4.4) van de beschouwingen van het hof waarin het vooral lijkt te gaan om het onrechtmatigheidsoordeel.
[302] Zie ook Menting 2015 en de noten onder dit arrest. HR 18 april 2014, ECLI:NL:HR:2014:942, JA 2014/65 m.nt. M.H.J. Lubbers & P. Oskam; JIN 2014/113 m.nt. R.D. Leen; JBPR 2014/49; NJ 2015/20 m.nt. M.M. Mendel en H.B. Krans (Achmea/Rijnberg). Zie ook de noten onder noot onder HR 11 juli 2014, ECLI:NL:HR:2014:1632 , JIN 2014/175 m.nt. P.C.M. Kemp, JBPR 2014/52 m.nt. M. Kremer.
[303] HR 18 april 2014, ECLI:NL:HR:2014:942, NJ 2015/20 m.nt. M.M. Mendel en H.B. Krans (Achmea/ Rijnberg)

gaat om de schending van de Gedragscode.[304] Krans merkt verder op dat wanneer een door een branche of partij zelf opgestelde code verder gaat dan waartoe het recht noopt, het volgens Krans minder voor de hand ligt een dergelijk gewicht aan schending van die code toe te kennen. Hij vervolgt dat indien schending van codes in het algemeen alleen aan de hand van een digitaal criterium (zwart-wit) wordt beoordeeld, het risico ontstaat dat hantering van codes niet aantrekkelijker wordt.[305] Ik deel deze laatste conclusie, maar ik zie niet in waarom het minder voor de hand ligt om minder gewicht toe te kennen aan schending van een code die door een branche of partij zelf is opgesteld. Het risico van het opstellen van een code lijkt mij te liggen bij de partij die hem opstelt. Daar komt bij dat het opstellen van een code zelden zonder zelfstandig belang is. Het opstellen van codes voor branches of partijen komt niet zelden tot stand onder dreiging van een toezichthouder of minister die anders tot wetgeving dreigt over te gaan. Er zitten voor partijen ook verschillende voordelen aan het opstellen van codes in vergelijking tot het opstellen van wetgeving, onder meer de flexibiliteit om in te spelen op ontwikkelingen in zowel de markt als het recht.[306] Zo kan het opstellen van een code ook economische voordelen bieden in termen van kosten of het aantrekken van nieuwe klanten. Veel codes horen met andere woorden bij het geheel van het recht waarin partijen zich bewegen op de markt. Het risico van minder gewicht toekennen aan codes is dat codes hun waarde verliezen. Het zou bovendien de (rechts)zekerheid van de wederpartij doen afnemen wanneer later zou blijken dat de waarde van de code zeer beperkt is. Anders dan Krans moet naar mijn mening geen bijzondere waarde worden gehecht aan het feit dat het in deze zaak een gedragscode betreft. Waar het hier om gaat is dat in de hier bedoelde gedragscode reeds alle rechtens relevante factoren ten aanzien van het rechtmatigheidsoordeel waren verdisconteerd waardoor het hof en de Hoge Raad bij het constateren van overtreding van de Gedragscode ook direct tot het oordeel konden komen dat er sprake was van onrechtmatig verkregen bewijs. Het oordeel zou naar mijn mening niet anders mogen uitvallen wanneer de rechter dezelfde situatie zou toetsen zonder gebruik te maken van deze Gedragscode. Het feit dat de Gedragscode zowel aandacht heeft voor het onrechtmatige karakter als voor de rechtvaardigingsgronden die het onrechtmatige karakter aan die daad kunnen ontnemen, leidt er in dit geval toe dat zowel het hof als de Hoge Raad de toets of er sprake is van onrechtmatig verkregen bewijs hieraan gelijk kan stellen. Nu zowel het hof als de Hoge Raad aan die beoordeling de conclusie verbinden dat dat gedrag niet beloond mag worden dringt de vraag zich op in welke gevallen een partij wel beloond mag worden wanneer hij bewijs op een onrechtmatige wijze heeft verkregen. In het licht van het eerder door de Hoge Raad gestelde belang van de waarheidsvinding zou het antwoord moeten luiden dat een partij dat alleen mag als hij de waarheid niet op een andere manier aan het licht kan brengen. In die zin is het niet onbegrijpelijk dat de Hoge Raad verwijst naar het oordeel van het hof dat

[304] HR 18 april 2014, ECLI:NL:HR:2014:942, NJ 2015/20 m.nt. M.M. Mendel en H.B. Krans (Achmea/ Rijnberg), ov. 3.4.6 en in Hof 's-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465. Krans in ov. 15.

[305] Deze mening wordt in alle genoemde annotaties gedeeld.

[306] Vgl. R. De Boer (directeur bij het Verbond van Verzekeraars) en Renée Martius (senior beleidsadviseur) in hun artikel 'Zelfregulering: een goed en betrouwbaar alternatief voor publieke regulering' in het Tijdschrift voor Financieel Recht 2014.

de verzekeraar ten onrechte verwijst naar het arrest L/Wennekes Lederwaren waarin de Hoge Raad van oordeel was dat inbreuk op privacyrechten gerechtvaardigd is wanneer er sprake is van een concreet vermoeden van strafbare feiten dat anders dan met gebruikmaking van een verborgen camera niet zou kunnen worden gestaafd.[307] Het hof betrekt dit oordeel bij de vraag of het onrechtmatig verkregen bewijs moest worden uitgesloten. Het kwam in deze zaak tot de conclusie dat de verzekeraar niet tot dit oordeel heeft kunnen komen en dat derhalve het bewijs moet worden uitgesloten. Met andere woorden nu de verzekeraar wel op een andere wijze de waarheid aan het licht had kunnen brengen en dit heeft nagelaten dient hem de onrechtmatige verkrijging van het bewijs te worden aangerekend en verbinden zowel het hof als de Hoge Raad daaraan de sanctie dat het onrechtmatig verkregen bewijs van het bewijs moet worden uitgesloten.

Ten tweede lijkt op het eerste gezicht de ernst van de inbreuk en de ernst van de gestelde fraude een rol te spelen bij het oordeel of onrechtmatig bewijs van het bewijs moet worden uitgesloten. De Hoge Raad komt tot het oordeel dat het hof beide omstandigheden in zijn oordeel betrokken heeft. Het hof betrekt in zijn oordeel duidelijk de beperkte ernst van de inbreuk op de privacyrechten van de verzekerde. Het leidt volgens het hof echter niet tot een ander oordeel. Minder duidelijk is de verwijzing naar de ernst van de gestelde fraude. De verzekeraar heeft in haar middel tot uitdrukking willen brengen dat de ernst van de gestelde fraude ertoe zou moeten leiden dat het onrechtmatig verkregen bewijs niet van het bewijs wordt uitgesloten. De Hoge Raad verwijst naar de hiervoor genoemde overweging waarin het hof onder verwijzing naar het arrest L/Wennekes Lederwaren tot de conclusie komt dat er geen sprake is van een concreet vermoeden van strafbare feiten en de verzekeraar dus ook geen gerechtvaardigd belang had om de privacyrechten van de verzekerde te schenden. In het arrest L/Wennekes Lederwaren speelt de ernst van de fraude in zoverre een rol dat de Hoge Raad de ernst van fraude voldoende acht om onder omstandigheden, namelijk dat er sprake is van een concreet vermoeden van strafbare feiten dat anders dan met gebruikmaking van een verborgen camera niet zou kunnen worden gestaafd, inbreuk op de privacyrechten van een medewerker rechtvaardig te achten. De ernst van de gestelde fraude is in die zin een conditie sine qua non. Wanneer de ernst van de gestelde fraude immers gering is kan er helemaal geen sprake van zijn dat de verzekeraar inbreuk maakt op privacyrechten van de verzekerde en dient het bewijs altijd te worden uitgesloten. De ernst van de fraude is daarmee een voorwaarde om onrechtmatig verkregen bewijs te kunnen gebruiken. Het hof betrekt de ernst van de fraude wel in zijn oordeel maar op een andere wijze dan de verzekeraar voor ogen had. De verzekeraar heeft hiermee immers vooral tot uitdrukking willen brengen dat de gestelde fraude dusdanig ernstig is dat uitsluiting van het bewijs niet op zijn plaats is. Het hof kwam met elementen uit het arrest L/Wennekes Lederwaren terecht tot een andere conclusie. De ernst van de fraude zal in de toekomst nauwelijks een rol meer spelen omdat Hoge Raad nu als uitgangspunt neemt dat onrechtmatig verkregen bewijs in beginsel toelaatbaar is, tenzij er

[307] Hof ‘s-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465 (Achmea/Rijnberg), ov. 37; HR 27 april 2001, ECLI:NL:HR:2001:AB1347, NJ 2001/421, m.nt. PAS (L/Wennekes Lederwaren).

sprake is van bijkomende omstandigheden.[308] De ernst van de fraude zou dan geen rol meer mogen spelen omdat dit slechts een argument vormt om het bewijs toe te laten en het toelaten van het bewijs thans het uitgangspunt vormt. Systematisch is er dan ook weinig reden om de ernst van de fraude te betrekken wanneer men de toelaatbaar van het bewijs als uitgangspunt neemt.

Samenvattend deel ik de mening van de annotatoren dat dit arrest niet heel veel duidelijkheid schept. Ik zal mijn oordeel verder uiteenzetten en mij daarbij beperken tot de voor watermerken relevante inbreuk op het recht van privacy.[309] De Hoge Raad stelt de waarheidsvinding en daarmee het toelaten van bewijs terecht voorop. Uitsluiting is derhalve slechts mogelijk indien er sprake is van bijkomende omstandigheden.[310]

De Hoge Raad maakt duidelijk een keuze voor het toelaten van het bewijs omwille van de waarheidsvinding. Hij sluit daarmee aan bij het idee van onder meer Kremer dat het algemene maatschappelijke belang dat de waarheid in rechte aan het licht komt in beginsel zwaarder weegt dan het belang van uitsluiting van bewijs. Anders dan Kremer acht de Hoge Raad uitsluiten van het bewijs onder omstandigheden wel mogelijk.[311] Al wordt in het arrest van de Hoge Raad niet duidelijk onder welke omstandigheden dit het geval is. Embregts stelt in haar proefschrift niet expliciet de waarheidsvinding voorop maar komt met een model dat het traditionele onderscheid naar rechtsgebied los laat en volgens haar de rechter handvatten biedt om in het spanningsveld van waarheidsvinding en rechtsbescherming tot een rechtvaardige en gemotiveerde beslissing te komen.[312] Zij benadert de toelaatbaarheid van onrechtmatig verkregen bewijs vanuit een grondrechtelijke invalshoek en constateert dat die invalshoek in het civielrecht en strafrecht niet tot een wezenlijke andere uitkomst zal leiden.[313]

Kremer en Embregts hebben zich vooral gericht op de vraag naar de grondslag van de bewijsuitsluiting. Kremer komt daarbij tot de conclusie dat bij gebrek aan een overtuigende grondslag bewijsuitsluiting als rechtsgevolg van onrechtmatig verkregen bewijsgaring als hoofdregel lastig te onderbouwen is. Hij kiest er dan voor om aan de begane onrechtmatigheid ‘gewoon’ het rechtsgevolg te verbinden dat volgens hem voortvloeit uit de regels van het materiële aansprakelijkheidsrecht, namelijk de verplichting tot het vergoeden van de schade

[308] Vgl. A-G Vranken voor HR 12 februari 1993, ECLI:NL:HR:1993:AJ8237 (W./gemeente Spijkenisse), ov. 29-30 die tot de conclusie komt dat W. geen bijzondere omstandigheden heeft aangevoerd die uitsluiting van het bewijs rechtvaardigen. Volgens Vranken wijst niets erop dat zijn belangen ontoelaatbaar zijn geschaad, terwijl daartegenover het grote belang van de gemeente staat om toe te zien op een juiste uitvoering van de ABW en het tegengaan of opsporen van fraude. Vranken merkt wel op dat ‘hier wellicht anders over geoordeeld moeten worden wanneer art. 84d lid 3 ABW het inwinnen van inlichtingen afhankelijk had gesteld van toestemming of medewerking van de betrokkene, maar als gezegd is dat niet het geval’.
[309] Zowel Kremer 1999 (diss.), p. 68 als Embregts 2003 (diss.), p. 58 komen tot de conclusie dat het bij onrechtmatige informatiegaringsmethoden in nagenoeg alle gevallen gaat om inbreuk op privacyrechten.
[310] HR 18 april 2014, ECLI:NL:HR:2014:942, ov. 5.2.3.
[311] Kremer 1999 (diss.), p. 304.
[312] Embregts 2003 (diss.), p. 295.
[313] Embregts 2003 (diss.), p. 331. Zij richt zich na die conclusie dan ook op de consequenties voor het bestuurs-recht.

ex. 6:162 BW. De schadevergoeding prevaleert voor Kremer boven de bewijsuitsluiting omdat de beoogde doelen die gepaard gaan met deze uitsluiting evengoed bewerkstelligd kunnen worden met het vergoeden van de schade en daar verder volgens hem niet de nadelen van bewijsuitsluiting aan kleven.[314] Embregts komt tot de conclusie dat er voldoende grond is om bewijs onder omstandigheden uit te sluiten. Wanneer de rechter heeft vastgesteld dat de uitsluitingsregel toepasselijk is dan kan volgens haar de uitsluiting ervan achterwege blijven wanneer is voldaan aan de relativeringen die op de bewijsuitsluitingsregel zijn aangebracht.[315] In dat kader wijst zij op de relativiteit, causaliteit en schade.[316] Bewijsmateriaal dat op een bijzonder onrechtmatige wijze is verkregen kan in het algemeen niet meewerken aan het bewijs.[317] Nu de Hoge Raad gekozen heeft om het algemene maatschappelijke belang dat de waarheid in rechte aan het licht komt, alsmede het belang dat partijen erbij hebben hun stellingen in rechte aannemelijk te kunnen maken, in beginsel zwaarder wegen dan het belang van uitsluiting van bewijs komt het nu aan op de vraag onder welke bijkomende omstandigheden het uitsluiten van het bewijs gerechtvaardigd is. De vraag onder welke omstandigheden het bewijs moet worden toegelaten lijkt daarmee niet langer relevant.[318]

De vraag die dan moet worden beantwoord is onder welke bijkomende omstandigheden het bewijs zou moeten worden uitgesloten. Uitsluiting van het bewijs zou naar mijn mening in het licht van de waarheidsvinding, evenals in het strafrecht het geval is, slechts een ultimum remedium moeten zijn. Hierbij moet worden gedacht aan die gevallen waarin het handelen van de partij die het onrechtmatig verkregen bewijs wil gebruiken echt onaanvaardbaar zou zijn.[319] Bijvoorbeeld bij ernstige schending van processuele belangen, ernstige inbreuk op het recht op de persoonlijke levenssfeer of handelingen die in strijd zijn met het strafrecht.[320] Daarbij kan worden gedacht een schending van de privacy waarbij strafrechtelijke normen worden geschonden, zoals hacken (art. 138ab Sr; computervredebreuk).[321] Asser wijst er terecht op dat vertrouwelijke informatie steeds gemakkelijker in handen te krijgen is met behulp van het internet en de wijze waarop tegenwoordig verschillende bestanden gekoppeld zijn. Een handige hacker die wordt ingehuurd om een proces te winnen kan op die manier een

[314] Zie uitgebreid Kremer 1999 (diss.), p. 301.
[315] Embregts 2003 (diss.), p. 301.
[316] Embregts 2003 (diss.), p. 245.
[317] Embregts 2003 (diss.), p. 301.
[318] Voor de volledigheid merk ik op dat ik hierna het geldende positieve recht volg zoals door de Hoge Raad uiteengezet in het arrest Achmea/Rijnberg. De lijn Embregts die van precies het omgekeerde startpunt uitgaat, zal hiermee verder niet meer vervolgd worden, omdat zij de toelaatbaarheid van onrechtmatig verkregen bewijs vanuit een grondrechtelijke invalshoek bekijkt. Ook zij constateert zelf dat die invalshoek in het civielrecht en strafrecht niet tot wezenlijke andere uitkomst zal leiden.
[319] Zie o.m. Plv. P-G De Vries Lentsch-Kostense ECLI:NL:PHR:2014:77, ov. 18 voor HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), onder verwijzing naar Van Dort 2000-1/2, p. 6 en Asser, 1999, p. 3.
[320] Zie ook Asser 2013, nr. 148, p. 160.
[321] Zie o.m. Embregts 2003 (diss.), p. 255 onder verwijzing naar Van Soeren 1986. Plv. P-G De Vries Lentsch-Kostense ECLI:NL:PHR:2014:77, ov. 18 voor HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg), onder verwijzing naar Van Dort 2000, p. 6 en Asser 1999-1, p. 3. Zaken zoals foltering vallen ook af omdat zij niet bijdragen aan het vinden van de waarheid (Shane O'Mara 2009). Strafrechtelijke vervolging, vanwege het feit dat een burger in strijd met het strafrecht bewijs heeft verzameld, komt weinig voor. Brouwer (2008, p. 106) concludeert dat de kern van het probleem eerder ligt in de vervolgingspraktijk dan in het gebrek aan een wettelijk instrumentarium.

partij van kennis voorzien die nodig is voor het bedenken van een goede processtrategie. Daarvoor hoeven de gegevens, zo stelt Asser terecht, niet eens in de procedure te worden gebracht.[322]

Wanneer het uitsluiten van het bewijs niet op deze grond kan plaatsvinden komt de rechter toe aan een afweging van belangen tegen de achtergrond dat het uitgangspunt is dat bewijs omwille van de waarheidsvinding toelaatbaar is.[323] Daarbij moet worden opgemerkt dat iedere afweging in dit leerstuk afhankelijk is van de omstandigheden van het geval waardoor het lastig is om algemene criteria te geven.[324] De belangrijkste vraag die moet worden beantwoord is of de geschonden norm het belang van de betrokkenen beoogt te beschermen.[325] Het gaat hier volgens Asser om de strekking van de door de onrechtmatige verkrijging geschonden norm in verhouding tot het gebruik van de door de schending verkregen informatie.[326] Asser noemt als voorbeeld dat diefstal van gegevens die niet bestemd zijn voor publicatie maar op zichzelf vatbaar zijn voor overlegging in een proces, op zichzelf niet snel uitsluiting van die informatie opleveren. Maar wanneer de diefstal ook inbreuk maakt op een norm die erop gericht is de informatie in rechte tegen openbaarmaking te beschermen dan ligt uitsluiting meer in de lijn der verwachting.[327] Hierbij kan ook worden gedacht aan informatie die verkregen is bij geheimhouders met een verschoningsrecht die deze informatie zelf nooit zouden hebben hoeven verstrekken.[328] Ook in dit geval beoogt de geschonden norm het belang van de betrokkenen te beschermen. In andere gevallen waarbij het verschoningsrecht geen gelding heeft wijst Asser erop dat van belang kan zijn in hoeverre de partij die slachtoffer is geworden van de onrechtmatige bewijsvergaring bevoegd was de informatie openbaar te maken.[329] Als dat het geval is, bijvoorbeeld wanneer het gaat om de eigen privacy, doet zich de vraag voor of de partij informatie die voor de beslissing van belang kan zijn op grond van art. 21 Rv (waarheidsplicht) niet zelf in het geding had moeten brengen. Behoudens zeer privacygevoelige informatie moet die informatie volgens Asser in het geding worden gebracht.[330] Wanneer de bevoegdheid tot openbaarmaking ontbreekt dan zal de rechter een afweging moeten maken tussen het belang van de waarheidsvinding en het geheim houden van de informatie. Ook in dat geval kan uitsluiting van het bewijs op zijn plaats zijn. Bij watermerken zal daarvan geen sprake zijn. De licentienemer is bevoegd om deze gegevens te openbaren en de gegevens zelf zijn niet zo gevoelig dat het belang van de waarheidsvinding daarvoor zou moeten wijken.

[322] Asser 2013, nr. 143, p. 156.
[323] Zie ook Embregts 2003 (diss.), p. 254 die opmerkt dat behoudens Kremer 1999 (diss.) (p. 272) in de literatuur voornamelijk een belangenafweging als maatstaf wordt verdedigd. Dat is ook anno 2015 nog steeds het geval.
[324] Zie ook Asser 2013, nr, 148, p. 159.
[325] Zie o.m. Embregts 2003 (diss.), p. 246; Asser 2013, nr. 148, p. 159.
[326] Asser 2013, nr. 148, p. 159.
[327] Asser 2013, nr, 148, p. 160.
[328] Idem.
[329] Asser 2013, nr, 148, p. 161.
[330] Idem.

Uitsluiting van het bewijs kan naar mijn mening ook plaatsvinden wanneer een partij bij herhaling heeft laten zien geen acht te slaan op bescherming van privacy van de wederpartij of de groep waartoe hij behoort. De rechthebbende, een verzekeraar of werkgever die in een vergelijkbaar geval reeds in een eerdere procedure(s) door de rechter is gewezen op het schenden van de privacy van de licentienemer en geen maatregelen treft om inbreuk op privacyrechten te voorkomen dan wel voortdurend weigert om het bewijs op een minder bezwarende of ingrijpende wijze te verzamelen (subsidiariteit) of acht te slaan op het beginsel van proportionaliteit neemt daarmee het risico dat het bewijs in een volgende procedure van het bewijs moet worden uitgesloten. In het licht van de vraag of onrechtmatig verkregen bewijs voor het bewijs mag worden gebruikt wijst Asser er nog op dat de anonimiteit van de bron nog een obstakel kan zijn voor de toelating van informatie, wanneer een partij geen mogelijkheid heeft de juistheid van de ingebrachte informatie te bestrijden.[331] Het is niet ondenkbaar dat deze problematiek een grotere rol gaat spelen in de toekomst, omdat bijvoorbeeld informatie die lang geleden is gedeeld via email of een andere berichtenservice (bv. Whatsapp) lastig te achterhalen is. Bij watermerken is dit denkbaar wanneer de rechthebbende bijvoorbeeld de identiteit van de licentienemer baseert op een Facebook-, Google-, of Microsoftprofiel en de licentienemer niet in staat is om (al dan niet via de rechthebbende) de benodigde gegevens bij deze ondernemingen te krijgen. Eenzelfde situatie is denkbaar wanneer bewijs dat is verkregen via een strafrechtelijk zaak gebruikt wordt in een civiele zaak. Zo zal de politie in de regel al dan niet met een rechterlijk bevel een betere toegang hebben tot bijvoorbeeld servers van de voornoemde organisaties. Het verzamelen of controleren van informatie door onderzoek te verrichten op bijvoorbeeld de server van die bedrijven zal in de praktijk lastig zijn. Nog daar gelaten dat bewijs dat via inlichtingendiensten is verzameld en waar nauwelijks controle op is via een strafzaak ook in het civiele proces kan worden gebruikt. Hiermee is vanzelfsprekend niet gezegd dat al dit bewijs onbetrouwbaar is. Het lijkt mij in de praktijk in ieder geval lastig om aan te tonen dat het onbetrouwbaar is.

Kremer stelt zich in zijn annotatie, evenals in zijn proefschrift, de vraag of bewijsuitsluiting eigenlijk wel de meest voor de hand liggende reactie is op onrechtmatige bewijsverkrijging? Hij beantwoordt de vraag in deze annotatie niet, maar laat onder verwijzing naar de voorzieningenrechter in Amsterdam wel zien dat het anders kan.[332] De rechter laat in deze arbeidszaak het bewijs toe en kent een schadevergoeding toe aan de werknemer, omdat volgens de rechter voorkomen moet worden dat het recht op privacy van een werknemer door het (onbelemmerd) gebruik van onrechtmatig verkregen bewijs ernstig zou worden uitgehold. Volgens de rechter ontstaat erop deze wijze ‘geen vrijbrief voor de werkgever om op onrechtmatige wijze gegevens te verkrijgen over een bepaalde handelwijze van een werknemer en blijft het tegelijkertijd mogelijk het gedrag van de werknemer te beoordelen

[331] Asser 2013, nr. 148, p. 160; HR 11 juli 2008, ECLI:NL:HR:2008:BC8421, NJ 2009, 451 m.nt. Dommering (De Telegraaf).
[332] HR 11 juli 2014, ECLI:NL:HR:2014:1632, JBPR 2014/52 m.nt. M. Kremer; Rb. Amsterdam van 12 mei 2014, ECLI:NL:RBAMS:2014:2751, JAR 2014/149, m.nt. C.M. Jakimowicz , ov. 21-22.

met alle gegevens die boven tafel zijn gekomen'.[333] Kremer liet in zijn proefschrift al eerder zien relevant en betrouwbaar bewijs mede omwille van de waarheidsvinding altijd toe te willen laten en 'aan de begane onrechtmatigheid 'gewoon' het rechtsgevolg te verbinden dat voortvloeit uit de regels van het materiële (aansprakelijkheids)recht, te weten het ontstaan van de verplichting tot het vergoeden van de daardoor geleden schade ex. 6:162 BW.'[334] Deze stelling van Kremer gaat mij een brug te ver en is in het algemeen ook niet zonder problemen, zoals Vranken terecht aangeeft in zijn bespreking van deze dissertatie.[335] Niettemin lijkt het leerstuk van het onrechtmatig verkregen bewijs, zoals Kremer in zijn dissertatie al aangaf, teveel toegespitst op de wenselijkheid van bewijsuitsluiting.[336] Kremer wijst in zijn dissertatie terecht op andere mogelijkheden zoals de meer gedifferentieerde sanctionering zoals deze in het strafrecht in artikel 359a Sv in de wet zijn neergelegd.[337] Het gaat mij hier om het idee van gedifferentieerde sanctionering en niet om het kopiëren van deze strafrechtelijke regeling naar het civiele recht.[338] Anders dan Kremer ben ik dus niet bereid om relevant en betrouwbaar bewijs altijd toe te laten en de begane onrechtmatigheid te compenseren van door middel van een schadevergoeding. Grove schendingen van het recht dienen mijns inziens altijd tot uitsluiting van het bewijs te leiden. In de praktijk zullen die gevallen, naar mijn verwachting, niet vaak voorkomen. Dit betekent echter niet dat er niet ook (andere) sancties, zoals het veroordelen tot het betalen van een schadevergoeding, kunnen zijn voor degene die in strijd handelt met de privacyrechten van een ander. Daarmee komen er ten minste twee categorieën sancties, namelijk het uitsluiten van het bewijs in die gevallen waarin er sprake is van grove schending van het recht en een andere categorie sancties, zoals bijvoorbeeld het laten betalen van een schadevergoeding, voor die gevallen waarin een partij in strijd gehandeld heeft met het (privacy)recht. Vanzelfsprekend kan van deze laatste categorie alleen sprake zijn wanneer de inbreuk niet zodanig grof is dat bewijsuitsluiting op zijn plaats is.

Het is mij onduidelijk of Kremer nog steeds van mening is dat ieder relevant en betrouwbaar bewijsmiddel moet worden toegelaten en de begane onrechtmatigheid in alle gevallen kan worden gecompenseerd door middel van een schadevergoeding. In de eerder genoemde annotatie wijst Kremer erop dat zich het merkwaardige fenomeen voordoet dat de civiele rechter, waar dat niet voor de hand ligt, een strengere norm aanlegt dan de strafrechter.[339] Volgens Kremer is men in het strafrecht allang af van de gedachte, dat wanneer de overheid

[333] Rb. Amsterdam van 12 mei 2014, ECLI:NL:RBAMS:2014:2751, JAR 2014/149, m.nt. C.M. Jakimowicz , ov. 21-22.
[334] Kremer 1999 (diss.), p. 305.
[335] Vranken 2000. Vranken stelt o.m. de vraag wat schadevergoeding voor zin heeft wanneer het gaat om een onrechtmatig bewijs in een zaak over een omgangsregeling. Heeft de betrokkene dan wel vermogensschade? Vranken denkt ook dat Kremer onderschat tot welke uitwassen zijn opvatting zal leiden, omdat er een premie wordt gezet op het met alle mogelijke middelen naar zich toe trekken van het processuele gelijk. Zie ook Embregst 2003 (diss.), p. 266.
[336] Kremer 1999 (diss.), p. 305. Ook Embregst 2003 (diss.) richt zich voornamelijk op het uitsluiten van het bewijs. Al geeft zij aan dat de schadevergoeding nog wel bestaat naast de bewijsuitsluitingsregel (p. 267).
[337] Kremer 1999 (diss.), p. 297-302.
[338] Zie later ter vergelijking het Belgisch recht, waarbij men ervoor gekozen heeft om het in de jurisprudentie van het Hof van Cassatie in 2003 ontwikkelde leerstuk van het ongeoorloofde bewijs in het strafrecht letterlijk over te zetten naar het civiele recht.
[339] Kremer verwijst hierbij naar het arrest HR 18 april 2014, ECLI:NL:HR:2014:942 (Achmea/Rijnberg).

zich niet aan haar eigen regels houdt, het uitsluiten van het bewijs in alle gevallen de meest voor de hand liggende sanctie is. Hij stelt dat 'zeker bij geringe rechtsinbreuken die zich op die wijze laten compenseren, wordt in het strafrecht veelal voor strafvermindering gekozen, hetgeen art. 359a Sv al sinds 1996 mogelijk maakt.' Het is mij niet duidelijk of Kremer in zijn annotatie tot uitdrukking heeft willen brengen dat hij is afgestapt van het idee dat hij verdedigde in zijn proefschrift, namelijk dat relevant en betrouwbaar bewijs mede omwille van de waarheidsvinding altijd moet worden toegelaten of dat hij slechts tot uitdrukking heeft willen brengen dat het toewijzen van schadevergoeding in sommige gevallen ('zeker bij geringe rechtsinbreuken') een goed alternatief is. Dat laatste ben ik zeker met hem eens.

De uitkomst van het arrest Achmea/Rijnberg roept, zoals Kremer terecht stelt, de vraag op of in dit geval uitsluiting van het bewijs de meest passende sanctie is.[340] Het antwoord op die vraag zal afhangen van het doel dat je nastreeft met het uitsluiten van het bewijs. Wanneer de rechters tot uitdrukking hebben willen brengen dat de verzekeraar zich aan privacyregelgeving moet houden dan lijkt bewijsuitsluiting op zijn plaats, omdat ik het niet waarschijnlijk acht dat een verzekeringsmaatschappij haar houding verandert omdat er in één zaak een schadevergoeding moet worden uitbetaald. Het honoreren van het verweer van de verzekeraar dat zij een groot belang heeft bij het opsporen van fraude komt er per saldo op neer dat de weg wordt vrijgemaakt voor een weinig zorgvuldige belangenafweging waardoor de privacyrechten van in dit geval de verzekerde snel in het geding zullen komen. Daarbij komt dat het belang van het vaststellen van fraude groot is, maar uitgaat van de gedachte dat de verzekerde ook daadwerkelijk de fraude heeft gepleegd. Wanneer men de zaak bekijkt vanuit de invalshoek van een onschuldige dan verandert de zaak van kleur. Het is niet ondenkbaar dat het hof en de Hoge Raad een signaal hebben willen afgeven dat de bescherming van privacy van belang is, ook omdat niet iedere verdachte het ook daadwerkelijk heeft gedaan. In die zin kan ik mij ook bij watermerken voorstellen dat de rechter onder omstandigheden bewijs dat in strijd met privacyrechten is verkregen van het bewijs uitsluit. Ook in het geval dat de inbreuk op het privacyrecht beperkt is gebleven.
In de regel zal de bescherming van privacy het terecht afleggen tegen het belang van de waarheidsvinding. Om recht te doen aan het beschermen van privacy moet worden voorkomen dat dit grondrecht wordt uitgehold en haar waarde verliest door het handelen in strijd met privacyrechten onbesproken te laten.[341] Het toewijzen van een schadevergoeding lijkt daarvoor de meest aangewezen sanctie om kenbaar te maken dat het een partij niet is toegestaan om informatie op een onrechtmatige wijze te verkrijgen.[342] Het op deze manier sanctioneren van een onrechtmatige daad past in het systeem van het recht en maakt het tevens mogelijk om recht te doen aan het uitgangspunt dat de waarheid in rechte aan het licht moet komen en dat partijen hun stellingen in rechte aannemelijk moeten kunnen maken.[343]

[340] HR 11 juli 2014, ECLI:NL:HR:2014:1632, JBPR 2014/52 m.nt. Kremer.
[341] Vgl. Koops & De Hert 2001 die erop wijzen dat het belang van privacy niet moet worden onderschat en privacy nog steeds een grondrecht is.
[342] Zie in de lagere rechtspraak o.m. Rb. Amsterdam 30 augustus 2010, ECLI:NL:RBAMS:2010:BP1423, ov. 12; Rb. Amsterdam 12 mei 2014, ECLI:NL:RBAMS:2014:2751, AR 2014/149 m.nt. C.M. Jakimowicz, ov. 21.
[343] Kremer 1999 (diss.), p. 305.

Anders dan Kremer ben ik van mening dat bewijs onder omstandigheden altijd moeten kunnen worden uitgesloten. Bijvoorbeeld in die gevallen waarin strafrechtelijke normen worden geschonden of een partij bij herhaling heeft laten zien geen acht te slaan op bescherming van privacy van de wederpartij of de groep waartoe hij behoort. De rechthebbende (of werkgever) die al in een eerdere procedure door de rechter is gewezen op het schenden van de privacy van de licentienemer neemt daarmee het risico dat het bewijs in een volgende procedure tegen een andere licentienemer wel wordt uitgesloten.
Door de rechter duidelijk meer mogelijkheden te bieden dan het uitsluiten van het bewijs kan het recht op privacy beter worden gewaarborgd. Ik acht het niet onvoorstelbaar dat de rechter met het oog op de waarheidsvinding ervoor kiest om reeds bij de vraag of bewijs is verkregen in strijd met privacyrechten tot het oordeel te komen dat er niet in strijd met de privacyrechten is gehandeld.[344] Daarmee komt de rechter immers niet toe aan de vraag of het verkregen bewijs van het bewijs moet worden uitgesloten. Door andere sancties, zoals schadevergoeding, mogelijk te maken kan worden voorkomen dat partijen het privacyrecht uithollen doordat zij altijd gebruik kunnen maken van bewijs dat zij in strijd met het privacyrecht hebben verkregen. Tegelijk wordt hiermee voorkomen dat de waarheidsvinding gevaar loopt doordat het bewijs moet worden uitgesloten. Door meer aandacht te hebben voor de mogelijkheid om onrechtmatig verkregen bewijs op een wijze te sanctioneren die de waarheidsvinding niet schaadt, ontstaat er ook meer ruimte voor nieuwe ontwikkelingen. Op deze manier kunnen gedragscodes of nieuwe technieken worden ontwikkeld en in de rechtspraak worden getoetst zonder dat de organisaties direct worden gesanctioneerd voor hun poging nieuwe wegen te bewandelen. De rechter dient naar mijn mening wel steeds te motiveren waarom onrechtmatig verkregen bewijs in een procedure wel of niet wordt toegelaten en wanneer hij het bewijs toelaat waarom er wel of geen sanctie wordt verbonden aan de onrechtmatige bewijsvergaring.

5.4.2.2 België

Tot 2003 was het algemene uitgangspunt in België dat onrechtmatig verkregen bewijs in beginsel niet in rechte kan worden aangewend en derhalve was uitgesloten van bewijs.[345] Met het Antigoon-arrest veranderde in 2003 de wijze waarop met onrechtmatig verkregen bewijs wordt omgegaan.[346] In een aantal arresten oordeelde het Hof eerst dat bewijs in strafzaken in beginsel onrechtmatig is wanneer het verkregen is op grond van een (1) misdrijf, (2)

[344] Visser (2008, p. 1923) merkt op dat verschillende rechters hebben aangegeven weleens een onjuiste motivering te hebben gebruikt voor een overigens juiste beslissing. Zie ook par. 4.2.3.2.
[345] Voor het eerst geintroduceerd door het Hof van Cassatie in 1923 (Cass. 12 maart 1923, Pas.1923, I, 233; Cass. 10 december 1923, Pas. 1924, I, 67) en later expliciet door het Hof (Cass. 18 april, 1985, Arr.Cass. 1984-85, 1102) toegepast in civiele zaken; Allemeersch & Schollen, p. 50. Niettemin was er verdeeldheid in de lagere rechtspraak. Waar een deel van de rechtspraak al wel rekening hield met omstandigheden van de zaak. Zie ook Allemeersch & Van Orshoven 2011, p. 76; Laenens e.a 2012, p. 550.
[346] Cass. 14 oktober 2003, P.030762.N, Arr.Cass. 2003, 1856, RABG 2004, 345 (Antigoon I); Cass. 23 maart 2004, AR. P.04.0012.N, RABG 2004, 1061, m.nt. F. Schuermans (Antigoon II). Het arrest heeft tevens de goedkeuring verkregen van het EHRM 28 juli 2009, ECLI:XX:BK4631, RABG, 2010/1, m.nt. F. Schuermans (Lee Davies/België) en Belgische Grondwettelijk Hof: GwH 22 december 2010, nr. 158/2010, JLMB 2011, 298. Van Compernolle 2011, p. 14-15; Allemeersch & Ryelandt, JT 2012, p. 167.

miskenning van regels van strafprocesrecht, (3) schending van privacy, (4) miskenning van het recht van verdediging of (5) het recht op menselijke waardigheid.[347] Het gebruik van onrechtmatig bewijs is thans enkel uitgesloten van bewijs wanneer (1) de overtreden norm of formaliteit op straffe van nietigheid is voorgeschreven; (2) de onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast en (3) het recht op een eerlijk proces is geschaad.

Zowel in de praktijk van de advocatuur als in de literatuur werd de toepassing van de Antigoonrechtspraak in het civielrecht bepleit.[348] Sinds 2008 worden de regels van dit arrest ook toegepast in burgerlijke zaken.[349] Evenals in het eerste arrest van 1923, waarin het Hof van Cassatie de eerste uitsluitingsregel introduceerde, volgt het civiel recht ook hier enkele jaren later het strafrecht.[350] De leer wordt ook door de feitenrechters inmiddels aanvaard.[351] In de eerste civiele zaak had het Arbeidshof een beslissing van de Rijksdienst voor Arbeidsvoorziening (RVA) om iemand van een uitkering uit te sluiten onwettig verklaard. De politie had in deze zaak een proces-verbaal naar aanleiding van een verhoor zonder toestemming van het OM naar de RVA doorgestuurd. Nu het proces-verbaal een akte is die onder het (strafrechtelijk gesanctioneerd) geheim van het strafonderzoek viel was het bewijs dat aan de beslissing ten grondslag lag onrechtmatig verkregen. Het Hof van Cassatie laat de beslissing of ongeoorloofd verkregen bewijs toelaatbaar is vervolgens aan de rechter. Het staat de rechter volgens het Hof, tenzij de wet het uitdrukkelijk anders bepaalt, vrij om de toelaatbaarheid van bewijsmateriaal te beoordelen in het licht van de artikelen 6 EVRM en 14 IVBPR. Op grond van de eerder genoemde Antigoonleer kan de rechter ieder onrechtmatig bewijs beoordelen in het licht van het doel van de geschonden norm op grond waarvan het bewijs is verkregen.[352] Dat geldt ook in het geval dat de schending niet het doel van de bescherming raakt die de wetgever aan de burger wilde verlenen.

De rechter dient volgens het Hof bij zijn oordeel rekening te houden met de omstandigheden van het geval en in het bijzonder ‘op het zuiver formeel karakter van de onregelmatigheid, op het gebrek aan weerslag van het aangeklaagde gebrek op het recht of de vrijheid die door de overschreden norm zijn beschermd, op de omstandigheid dat de wederrechtelijke beoordeling die aan de politie of de aangever wordt toegeschreven niet opzettelijk is, dat het onrechtmatig verkregen bewijs slechts betrekking heeft op een materieel bestanddeel van het misdrijf of

[347] Voor een expliciete verwijzing naar het schenden van privacy zie o.m. Cass. 2 maart 2005, P.04.1644.F, Arr.Cass. 2005, 506, JLMB 2005, 1086 m.nt. M. Beernaert, Journal Proc. 2005, 499, 23, m.nt. P. Toussaint; CR 2005/41m p. 258-263, m.nt. Van Eecke en B. Ooma. (Chocolatier Manon) en par. 5.4.2.
[348] Allemeersch & Ryelandt, JT 2012, p. 167; Hendrickx 2006, p. 687 meent dat de Antigoonrechtspraak niet zonder meer is over te zetten naar de praktijk van het arbeidsrecht.
[349] Cass. 10 maart 2008, S.07.0073.N, Pas. 2008, I, 652, JLMB 2009, 580, m.nt. R. De Baerdemaeker, NjW 2010, 195, m.nt. K. Van Kildonck. Voor 2008 werd hier aan voorbij gegaan concludeert ook Van Kildonck, 2010, p. 181 onder verwijzing naar o.m. Arbh. Brussel 3 mei 2006, AR 45.922; Arbh. Brussel 15 juni 2006, JTT 2006, 392; Arbrb. Brussel 4 december 2007, JTT 2008, 179.
[350] Cass. 12 maart 1923, Pas.1923, I, 233; Cass. 10 december 1923, Pas. 1924, I, 67.
[351] Mougenout 2011, p. 593-606, p. 595; Cattoir 2013, p. 572.
[352] Cass. 10 maart 2008, S.07.0073.N, NjW 2010, 195. In de Vlaamse literatuur spreekt men ook wel van de finaliteit.

nog dat de onregelmatigheid die aan de vaststelling van het misdrijf voorafging of daarmee gepaard ging, volstrekt onevenredig is met de ernst van dat misdrijf'.

De eerste voorwaarde voor de straffe van nietigheid lijkt vooral een voorwaarde die in het strafrecht zijn toepassing vindt. In het civiele recht zijn immers nauwelijks bepalingen te vinden zijn die op straffe van nietigheid in de wet zijn opgenomen, zoals in het strafrecht waar op straffe van nietigheid voorwaarden zijn gesteld aan bijvoorbeeld een telefoontap.

Een paar maanden later komt er meer onzekerheid doordat de Franstalige kamer in een andere zaak arrest wijst waarin aanvaard wordt dat de rechter onrechtmatig verkregen bewijs niet toelaat zonder deze eerst aan de eerder genoemde Antigoon-normen te toetsen.[353]

> 'Het arrest, dat beslist dat de eiser, die, samen met anderen, zich de door hem voorgelegde brieven heeft toegeëigend "om er onregelmatige kopieën van te maken", "niet aantoont dat (hij) (deze) op regelmatige wijze in zijn bezit heeft", en dat de eiser weliswaar een onrechtmatig gebruik van die brieven verwijt, maar geen gebruiksdiefstal vaststelt en zich noch op het briefgeheim noch op het vertrouwelijk karakter van de betrokken brieven baseert, omkleedt zijn beslissing om die brieven uit het debat te weren, regelmatig met redenen en verantwoordt ze naar recht.'

Het Hof van Cassatie sluit daarmee aan bij een deel van de lagere rechtspraak en de literatuur waar de zaken al eerder waren verschoven van de vraag naar de geoorloofdheid naar de beoordeling van de sanctie.[354] Bewijs dat onrechtmatig is verkregen moet alleen geweerd worden wanneer dit wordt gebruikt door diegene die voor de onrechtmatigheid verantwoordelijk is.[355] Het Hof heeft met de uit het strafrecht 'geknipte' formulering aansluiting gezocht bij het strafrecht en lijkt daarmee tevens aansluiting te zoeken bij de daar verder ontwikkelde leer. In de literatuur is opgemerkt dat in de toekomst meer duidelijkheid verwacht wordt omdat het begrippenapparaat door het knip- en plakwerk niet overeenkomt met het civiele begrippenapparaat.[356] De meerderheid is in de literatuur van mening dat het Hof van Cassatie met het eerste arrest van 10 maart 2008 een principe uitspraak heeft gedaan. Waar voor 2008 de algemene regel was dat onrechtmatig verkregen bewijs in principe ontoelaatbaar was en slechts in uitzonderlijke gevallen toelaatbaar wordt de regel nu omgekeerd door onrechtmatig verkregen bewijs in principe toelaatbaar te achten, tenzij er sprake is van ten minste van één van de drie opgesomde voorwaarden. Hiermee zou dan zijn

[353] Cass. 10 november 2008, S.06.0029.F, JTT 2009, 18. (Arbeidszaak). Tussen deze zaak en de zaak van 10 maart 2008 zijn er met name in arbeidszaken wel arresten gewezen waarin de hoven op basis van deze laatste uitspraak (Antigoonprincipes) het bewijs niet uitsloten. Zie o.m. Arbh. Antwerpen (afd. Hasselt), 2 september 2008, AR 2070230, onuitg.; Arbrb. Gent 1 september 2008, AR 175054/06. Anders Arbrb. Luik 3 september 2008, AR 371.015, welke voor het weigeren van het bewijsmiddel verwijst naar een uitspraak van Arbh. Brussel 15 juni 2006 JTT 2006, 392 (en dus voor 10 maart 2006).
[354] Allemeersch & Van Orshoven 2011, p. 75.
[355] Allemeersch & Schollen 2002, p. 60; Allemeersch & Van Orshoven 2011, p. 73, 75. Cattoir 2013, p. 556.
[356] Allemeersch & Van Orshoven 2011, p. 76. Zie in het arrest zelf verwijzen naar 'de overheid die met opsporing, het onderzoek en de vervolging is belast'. Voor meer pijnpunten zie o.m. Wagner 2008, p. 171. En de verschillende noten onder het arrest van 10 maart 2008, Kefer in RCJB 2009, 325; De Baerdemaeker in JLMB 2009, 584. Zie voor een overzicht van de kritiek Cattoir 2013, p. 573. Mougenot 2011, p. 246. Ziet in dit arrest vooral een eenvoudige 'copy-paste' van de motivering uit de strafrechtelijke Antigoonrechtspraak.

gekozen voor het idee dat de waarheidsvinding moeten prevaleren boven het recht dat met de verkrijging van het bewijs is geschonden. Niettemin is er in het licht van het arrest van 10 november 2008 veel onduidelijk over de status van het arrest van 10 maart 2008. Mede omdat de Nederlandstalige afdeling van de derde kamer van het Hof van Cassatie in 2011 een arrest vernietigde dat het bewijs uit had gesloten vanwege de onrechtmatige verkrijging.[357] Zowel in het arrest van 10 november 2008 als in het arrest van 2011 verwijst het Hof van Cassatie niet naar zijn uitspraak van 10 maart 2008. Mougenot ziet geen werkelijke tegenstrijdigheid tussen beide arresten van het Hof van Cassatie, omdat het Hof volgens hem in het eerste arrest geen principe uitspraak doet.[358] De draagwijdte van dat arrest beperkt is volgens hem beperkt tot civiele zaken, zoals het arbeidsrecht, waarbij de grenzen worden bepaald door de openbare orde en het strafrecht. In de praktijk is het afwachten of het Hof van Cassatie in een nieuw arrest meer duidelijkheid schept. Evenals naar Nederlands recht is het lastig vast te stellen of het hoogste nationale rechtscollege met het nalaten van een verwijzing naar eerdere rechtspraak een duidelijke boodschap heeft.

Voor watermerken is het de vraag of en onder welke omstandigheden de Antigoon-normen tot de conclusie leiden dat het gebruik van het watermerk als bewijsmiddel ontoelaatbaar is. Ten eerste is er geen wetgeving van toepassing op het gebruik van het watermerk waarbij nietigheid als sanctie is voorgeschreven. Zo is er ook in het privacyrecht geen bepaling voorgeschreven op straffe van nietigheid. Bij de tweede norm die ziet op de aantasting van de betrouwbaarheid van het bewijsstuk is het van belang voorop te stellen dat de aantasting van de betrouwbaarheid een gevolg moet zijn van de verkrijgingshandeling.[359] Het schenden van het privacyrecht zal in beginsel geen invloed hebben op de betrouwbaarheid van de gegevens en zal dus niet snel leiden tot het uitsluiten van het watermerk als bewijsmiddel.[360] Uitgesloten is het echter niet omdat het gebrek aan het nemen van voldoende technische en organisatorische maatregelen ook kan leiden tot onbetrouwbaar bewijs. De rechter zal in die gevallen echter eerder aansluiten bij de onbetrouwbaarheid van het bewijs en het watermerk om die reden dan uitsluiten van het bewijs. Ten derde is het de vraag of de inzet van het watermerk het recht op een eerlijk proces verstoort. Zolang het recht op tegenspraak gerespecteerd wordt zal dit echter niet snel worden aangenomen.[361] Het is echter niet uitgesloten dat er sprake kan zijn van een miskenning van een regel van civiel bewijsrecht als de verdediging niet in staat is controle uit te voeren op de betrouwbaarheid van het watermerk.[362] Met betrekking tot privacy heeft ook de rechtspraak zich, ook na de Antigoon-

[357] Cass. 2 mei 2011, JTT 2011, 469.
[358] Mougenot 2011, p. 246. Vgl. Van Doninck 2011, p. 14.
[359] Traest 2004, p. 137. Arbeidshof Brussel, 2 mei 2011 achtte de geloofwaardigheid van verklaringen verkregen na schending van de privacy ongeloofwaardig en als gevolg van deze ongeoorloofde wijze van handelen verwerpt zij ook de bekentenis van de werknemer. In de meeste gevallen wordt de betrouwbaarheid van het bewijs aangetast, doordat de techniek vanuit wetenschappelijk oogpunt niet voldoende waarborgen
biedt of doordat de techniek niet correct werd toegepast. Kildonck 2010, p. 182
[360] Verhelst & Thoelen 2006, p. 205-206.
[361] Traest 2004, p. 137; Verhelst & Thoelen, p. 206.
[362] Hierbij kan worden gedacht aan het niet uitwisselen van informatie waardoor de wederpartij bepaalde stellingen niet kan weerleggen, bijvoorbeeld omdat slechts delen van een email ter beschikking zijn gesteld waardoor niet het hele verhaal of de context duidelijk wordt. Zie in dit licht in het strafrecht het recht van de

arresten, al op het standpunt gesteld dat een schending van privacy niet automatisch leidt tot schending van het recht op een eerlijk proces op grond van artikel 6 EVRM.[363] Dat betekent dat wanneer men ook in de lagere rechtspraak de lijn van het Hof van Cassatie volgt, het watermerk - ook in het geval dat er in een eerdere fase onrechtmatig is gehandeld – niet snel als bewijsmiddel wordt uitgesloten.

In de rechtspraak lijkt de beoordeling van de rechtmatigheid van bewijsmiddelen neer te komen op een evenredigheidstoets omdat het recht op privacy tegenover het recht op bewijs en het auteursrecht komt te staan. In de rechtspraak lijkt een evenredigheidstoets vooral te bestaan in vragen naar het doel van het middel, proportionaliteit van de maatregel die toereikend dient te zijn en niet overmatig. Daarbij kan ook rekening gehouden worden met het niet voorhanden hebben van alternatieve mogelijkheden van bewijsverkrijging.[364] Of daarvan sprake is, is afhankelijk van de omstandigheden van het geval. In dit kader worden zaken vaak ook aan artikel 8 EVRM getoetst. De hiervoor beschreven belangenafweging sluit tevens aan bij de meer algemene wijze waarop de vraag naar de (on)rechtmatigheid van verkregen bewijs in de rechtspraak wordt beoordeeld. Namelijk in het licht van een belangenafweging tussen enerzijds degene die zich op de onrechtmatigheid van het bewijs beroept en anderzijds het recht op bewijs of de waarheid van de tegenpartij, dat is afgeleid van het algemene rechtsbeginsel van het recht op verdediging.[365]

Tot slot is er de vraag of ook bewijsstukken die zijn verkregen als gevolg van het ongeoorloofd gebruik van het watermerk als bewijsstuk kunnen dienen (fruit of poisonous tree). Het is immers niet ondenkbaar dat men de vermeende inbreukmaker confronteert met het watermerk en dat de vermeende inbreukmaker daarna bereid is mondeling dan wel schriftelijk te erkennen zich schuldig te hebben gemaakt aan inbreuk op het auteursrecht. In beginsel geldt in deze situatie dat wanneer wordt vastgesteld dat een bepaald bewijsstuk ongeoorloofd is, alle bewijsstukken die zijn verkregen dankzij het ongeoorloofde bewijs moeten worden geweerd met inachtneming van de Antigoon-normen.[366]

Samenvattend kan worden gesteld dat anders dan de Nederlandse Hoge Raad het Hof van Cassatie niet expliciet een keuze voor de waarheidsvinding maakt. Evenals de Nederlandse Hoge Raad eerder deed voor zijn uitspraak van 11 april 2014, kiest het Hof van Cassatie voor een weg die er in de praktijk toe zal leiden dat dat onrechtmatig verkregen bewijs slechts in

verdediging om na te gaan of de procedurele regels zijn nageleefd. Cass. 24 april 1996, Cass. 1997, 15, m.nt. L. Arnou; Verstraeten 2012, p. 993.

[363] Cass. 2 maart 2005, P.04.1644.F, A.C. 2005, 506 (Chocolatier Manon); EHRM 12 mei 2000, NJCM Bulletin, p. 1255, m.nt. E. Myjer (Kahn/Verenigd Koninkrijk).

[364] Cass. 27 februari 2001, JT 2000-01, 949, m.nt. I. Verhelst, CR 2001, 202; J. Dumotier, RW 2001-02, 1171; P. Humblet en Vigiles 2001, 153, m.nt. P. De Hert.

[365] Allemeersch & Schollen 2002, p. 60; Allemeersch 2007, p. 410; Allemeersch & Van Orshoven 2011, p. 73, 75; Cattoir 2013, p. 567. Vgl. Cass. 25 september 2000, A.C. 2000, 1424; P&B 2001, 114, m.nt. B. Allemeersch. Zie voor het recht op verdediging voor 2003, Du Jardin, 2003 en in de strafzaken Cass. 20 november 2007, P.07.1173.N/4; Cass. 16 december 2008 P.2008.1210.N.

[366] Deze leer wordt ook wel aangeduid als de fruit of poisonous tree doctrine of het secundaire bewijs en is in Burgerlijke zaken door het Hof van Cassatie toegepast vanaf 18 april 1995 (Arr, Cass. 1984-85, 1102).

bijzondere situaties van het bewijs zal worden uitgesloten. Dit zal er ook in België toe leiden dat het watermerk niet snel als een ongeoorloofd bewijsmiddel uit de debatten zal worden geweerd. Ten eerste doordat de rechthebbende zelf op eenvoudige wijze kan voldoen aan de geldende privacyregelgeving door zijn gebruikers voor te lichten en voldoende technische en organisatorische maatregelen te nemen. Zelfs wanneer de rechter tot het oordeel komt dat het watermerk is verkregen in strijd met het privacyrecht zal het niet snel ontoelaatbaar worden geacht. De drempel om bewijs als ongeoorloofd aan te merken en uit de debatten te weren is sinds het Antigoon-arrest immers nog meer verhoogd. Van Kildonck stelt dat de betekenis van privacy 'wel degelijk belang houdt en er geen sprake is van een uitholling van het recht op privacy', omdat op verschillende schendingen nog wel strafsancties bestaan dan wel aanleiding geven tot een burgerlijke schadevergoeding. Vanuit de theorie is er weinig aan te merken op dit standpunt. In de praktijk is het alleen de vraag of dat standpunt standhoudt. Het antwoord op die vraag hangt immers sterk samen met de vraag hoe vaak er in dergelijke gevallen vervolgd wordt en in hoeverre er ook sancties worden opgelegd dan wel in civiele context er (verder) geprocedeerd wordt om deze burgerlijke schadevergoeding te verkrijgen. Die kans lijkt mij evenals naar Nederlands recht bijzonder klein en daarmee is het privacyrecht in de praktijk wel degelijk verder uitgehold.

5.5 Samenvatting en conclusies

Om als juridisch bewijs effectief te kunnen zijn zal het watermerk als juridisch bewijsmiddel moeten worden toegelaten in een procedure. Voor het antwoord op de vraag of daarvan sprake is zijn twee vragen van belang. Ten eerste de vraag of het watermerk als juridisch bewijsmiddel kan worden gekwalificeerd en ten tweede de vraag of eventuele inbreuken op rechten van de licentienemer uitsluiting van het bewijs tot gevolg heeft. Deze laatste vraag valt uiteen in de vraag naar de rechtmatigheid van het watermerk als bewijsmiddel en de eventuele uitsluiting daarvan als gevolg van onrechtmatig handelen van de rechthebbende.

De kwalificatie van watermerken als juridisch bewijsmiddel

Ten eerste is gekeken naar de vraag of het watermerk als een juridisch bewijsmiddel gekwalificeerd kan worden (par. 5.2). Het Nederlandse civiel recht kent evenals het Belgische strafrecht een open of vrij stelsel van bewijs op grond waarvan de rechter in beginsel ook zelf kan bepalen welke middelen hij toelaat. In het Belgische civiel recht wordt de rechthebbende, evenals in het Nederlandse strafrecht geconfronteerd met een gesloten stelsel van bewijsmiddelen. In de praktijk wordt dit gesloten stelsel in beide landen echter ruim geïnterpreteerd waardoor technische middelen wel als juridisch bewijsmiddel worden erkend. In zowel het Belgische civiel recht als in het Nederlandse strafrecht is in de literatuur ook wel gepleit voor een open of vrij stelsel van bewijs. Beide landen laten vanuit de praktijk zien dat een gesloten stelsel van bewijsmiddelen in de praktijk zoveel ruimte krijgt dat het watermerk als juridisch bewijsmiddel niet op deze kwalificatiekwestie wordt uitgesloten.

Watermerken als onrechtmatig verkregen bewijs

Ten tweede is gekeken naar de vraag of het watermerk als bewijsmiddel op een andere wijze ontoelaatbaar zou zijn. Daarbij is vooral gekeken naar de vraag of het watermerk is verkregen in strijd met privacyrechten van de licentienemer (par. 5.3). Eerst is gekeken naar de grondrechtelijke kaders rondom de inzet van techniek bij de handhaving van auteursrecht. Daarna is het (on)rechtmatige karakter van het watermerk als bewijsmiddel vanuit nationaal perspectief bekeken naar Nederlands en Belgisch civiel- en strafrecht.

In het arrest Scarlet/Sabam (2011) heeft het Europese Hof van Justitie EU een eerste beoordeling gegeven over de inzet van (filter)techniek bij de handhaving van het auteursrecht. Het Hof bespreekt in dat licht drie grondrechten: de vrijheid van ondernemerschap, het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken. Het Hof komt in deze zaak tot de conclusie dat het juiste evenwicht ontbreekt tussen enerzijds de bescherming van het intellectuele eigendomsrecht en anderzijds, het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken. Deze conclusie stelt ook grenzen aan de mogelijkheden om een watermerk in te zetten. De verschillen in object (filtersysteem versus watermerk) zijn afgezet tegen de criteria die het Hof hanteert en leiden tot de conclusie dat behoudens een mogelijke inbreuk op privacyrechten van de licentienemer er vooralsnog weinig reden is om aan te nemen dat het Hof afwijzend zou staan tegenover het gebruik van watermerken.

Reeds bij de opkomst van watermerken was er vanuit de Europese toezichthouder (werkgroep 29) aandacht voor privacy van licentienemers. In 2008 publiceerde de Amerikaanse burgerrechtbeweging Center for Democracy & Technology (CDT) hun eigen ‘Privacy Principles for Digital Watermarking’ waarmee het een concreet toetsingskader heeft ontwikkeld dat voldoet aan Europese privacyrichtlijnen en de implementatie daarvan in de Nederlandse en Belgische wetgeving. Deze beginselen vragen aandacht voor (1) Privacy by design, waarmee wordt bedoeld dat er vanaf het begin van de ontwikkeling aandacht moet zijn voor privacy; (2) het vermijden van direct bruikbare informatie, zodat zelfs wanneer de informatie openbaar wordt deze niet direct bruikbaar is; (3) het informeren van de gebruiker; (4) het beperken van de toegang tot het uitlezen van watermerken; (5) het adequaat reageren als de watermerkalgoritmen zijn gekraakt; (6) de bescherming van de databanken; (7) het beperken van het gebruik voor andere doeleinden en tot slot (8) de zorg voor toegang en wijzigingsmogelijkheden voor gebruikers. Het is onduidelijk of en zo ja welke van deze beginselen in de praktijk worden nageleefd en op welke wijze daaraan invulling wordt gegeven. Vanwege de beperkte inspanning, de kleine groep van leveranciers en de aandacht voor het watermerk als bewijsmiddel in zowel de praktijk als in de literatuur, ligt het in de lijn der verwachting, dat er aandacht is voor deze (privacyrechtelijke) vragen. Het CDT wees erop dat ondanks de inzet van watermerken zij niet bekend is met problemen rondom privacy of misbruik. De watermerken waar het CDT naar refereert werden echter op een veel kleinere

schaal ingezet dan de watermerken als bedoeld in dit onderzoek. Niettemin zijn ook bij de watermerken in dit onderzoek weinig problemen te verwachten.

Om na te gaan of en zo ja onder welke omstandigheden de rechthebbende bij het verwerken van gegevens in strijd handelt met de privacy van de licentienemer is gekeken naar de nationale privacywetten van beide landen die beiden mede hun oorsprong vinden in de privacyrichtlijn.

In beide landen geldt dat voor het verwerken en gebruiken van persoonsgegevens bij watermerken geen specifieke wettelijke grondslag bestaat, waardoor voor de beoordeling van de rechtmatigheid van de verwerking van deze gegevens nagegaan moet worden of bij het verwerken ervan in strijd gehandeld is met de algemene regels inzake privacy. Zowel de Nederlandse Wet bescherming persoonsgegevens (Wbp) als de Belgische Wet met betrekking tot de verwerking van persoonsgegevens (WVP) komen voor een belangrijk deel voort uit de Europese privacyrichtlijn en hebben om die reden vergelijkbare bepalingen ten aanzien van de voorwaarde waaronder de gegevens in het watermerk mogen worden verwerkt. Overtreding van de in deze wetten opgenomen zorgvuldigheidsnormen vormen dan ook een onrechtmatige daad. In het bijzonder moet hierbij worden gedacht aan de wijze waarop de persoonsgegevens worden verkregen, verwerkt en bewaard. Dat betekent onder meer dat persoonsgegevens op grond van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden dienen te worden verzameld en enkel verwerkt mogen worden als deze gelet op de doeleinden waarvoor ze worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. Voor watermerken is het van belang dat iedere verwerking gebaseerd moet zijn op een zogenoemde verwerkingsgrondslag. De ondubbelzinnige toestemming van de licentienemer is de meest voor de hand liggende grondslag voor de verwerking van persoonsgegevens. De rechthebbende zal in andere gevallen de licentienemer in ieder geval moeten informeren over de verwerking van de persoonsgegevens als ook over het doel ervan, inclusief eventuele doorgifte van zijn gegevens. Het nalaten hiervan kan leiden tot het oordeel dat er in strijd gehandeld is met de Wbp of WVP en dat daarmee inbreuk is gepleegd ten aanzien van de privacy van in dit geval de licentienemer. Het recht op privacy is in beide landen geen absoluut, maar een functioneel recht waarbij in het kader van de rechtmatigheid een balans moet worden gezocht tussen verschillende rechten van partijen. Wanneer de rechter tot de conclusie komt dat er sprake is van inbreuk op het privacyrecht van de licentienemer komt de rechter toe aan de vraag of de schending gerechtvaardigd was. De rechtvaardiging kan worden gevonden in criteria die zijn neergelegd in nationale privacywetten alsmede in artikel 8 EVRM. Bij watermerken zal de rechter verder een afweging moeten maken tussen enerzijds het belang van de licentienemer bij eerbiediging van zijn persoonlijke levenssfeer en anderzijds het belang van de rechthebbende bij het beschermen van zijn intellectuele eigendom. Bij de beoordeling van de ernst van de inbreuk kan ook de aard en de mate van intimiteit van de informatie van groot gewicht zijn. Bij het verwerken van eenvoudige en niet-bijzondere persoonsgegevens, zoals de NAW-gegevens zal de ernst van de inbreuk mede vanwege de aard en zeer beperkte mate van intimiteit gering worden geacht. Dat heeft tot

gevolg dat een inbreuk op de nationale privacywetten in de regel leidt tot de kwalificatie dat het bewijs op een onrechtmatige wijze is verkregen.

Gevolgen van onrechtmatig verkregen bewijs

Naar nationaal recht wordt in de literatuur het uitsluiten van bewijs in beide landen en beide onderzochte rechtsstelsels onder omstandigheden mogelijk geacht, maar in het kader van de waarheidsvinding en het recht op verdediging niet gezien als de meest wenselijke uitkomst. Om bewijs niet uit te sluiten heeft de rechter in beginsel twee mogelijkheden. Ten eerste kan de rechter de bedoelde handelingen niet onrechtmatig achten waardoor hij niet toe komt aan de vraag of het bewijs moet worden uitgesloten. Ten tweede kan de rechter de handeling als onrechtmatig beoordelen maar vervolgens in zijn afweging omstandigheden aanwijzen waardoor hij uitsluiting niet op zijn plaats acht. Ondanks dat het overtreden van de nationale privacyregelingen in beginsel een onrechtmatige daad oplevert leidt dit in de jurisprudentie in veel gevallen niet tot een dergelijke kwalificatie in de motivering bij de Hoge Raad en het Hof van Cassatie. In de lagere rechtspraak in Nederland is het beeld hetzelfde, zij het dat daar meer expliciet aandacht is voor belangenafweging, ook in het kader van de waarheidsvinding. De Nederlandse Hoge Raad heeft er recent in het arrest Achmea/Rijnberg expliciet voor gekozen dat in civiele zaken het algemene maatschappelijke belang dat de waarheid in rechte aan het licht komt in beginsel zwaarder weegt dan het belang van uitsluiting van bewijs. Het uitsluiten van het bewijs is volgens de Hoge Raad dan ook slechts gerechtvaardigd, indien sprake is van bijkomende omstandigheden. In België was voor 2008 de regel dat onrechtmatig verkregen bewijs in beginsel van het bewijs werd uitgesloten. Het gebruik van onrechtmatig bewijs is sinds 2008 enkel uitgesloten van bewijs wanneer (1) de overtreden norm of formaliteit op straffe van nietigheid is voorgeschreven; (2) de onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast en (3) het recht op een eerlijk proces is geschaad. Het recht op een eerlijk proces komt mede voort uit de Europese rechtspraak en geldt ook voor de beoordeling naar Nederlands recht als een ondergrens. Anders dan de Nederlandse Hoge Raad heeft het Hof van Cassatie in België niet expliciet duidelijk gemaakt dat de waarheidsvinding in beginsel zwaarder weegt dan het belang van uitsluiting van bewijs. Al wordt dit in de literatuur inmiddels wel aangenomen.

Kremer wijst in zijn dissertatie terecht op andere mogelijkheden zoals de meer gedifferentieerde sanctionering zoals deze in het strafrecht in artikel 359a Sv in de wet zijn neergelegd. In tegenstelling tot Kremer ben geen voorstander om relevant en betrouwbaar bewijs altijd toe te laten en de begane onrechtmatigheid te compenseren door middel van een schadevergoeding. Grove schendingen van het recht dienen mijns inziens altijd tot uitsluiting van het bewijs te leiden. Maar door andere sancties, zoals schadevergoeding, mogelijk te maken kan wellicht wel worden voorkomen dat partijen het privacyrecht uithollen doordat zij op grond van de huidige praktijk altijd gebruik kunnen maken van bewijs dat zij in strijd met het privacyrecht hebben verkregen. Tegelijk wordt hiermee voorkomen dat de waarheidsvinding gevaar loopt doordat het bewijs moet worden uitgesloten. Door meer

aandacht te hebben voor de mogelijkheid om onrechtmatig verkregen bewijs op een wijze te sanctioneren die de waarheidsvinding niet schaadt, ontstaat er ook meer ruimte voor nieuwe ontwikkelingen. Op deze manier kunnen gedragscodes of nieuwe technieken worden ontwikkeld en in de rechtspraak worden getoetst zonder dat de organisaties direct worden gesanctioneerd voor hun poging nieuwe wegen te bewandelen.

In het strafrecht is bij de vraag naar de toelaatbaarheid van watermerken de vraag centraal gesteld of het OM bewijs mag gebruiken dat door de rechthebbende op een onrechtmatige wijze is verkregen. Zolang de overheid geen bemoeienis heeft gehad met de onrechtmatige verkrijging van het bewijs, is er in de regel zowel naar Nederlands als Belgisch strafrecht geen reden zijn om aan te nemen dat onrechtmatig verkregen bewijs van het bewijs zal worden uitgesloten. Bij watermerken zal de overheid in de regel geen bemoeienis hebben met het aanbrengen van watermerken in content van private partijen. Evenals in het civiel recht zal ook in het strafrecht de betrouwbaarheid van het bewijs een grotere rol spelen dan de vraag naar de juridische toelaatbaarheid. Een verweer dat gericht is op het uitsluiten van het watermerk voor het bewijs zal zowel naar Nederlands als Belgisch civiel- en strafrecht dan ook weinig kans van slagen hebben.

In de literatuur blijft de vraag wat er nog van het grondwettelijk bewijsrecht overblijft als aan de schending van de norm geen directe sancties worden verbonden, mede in het licht van een eerlijk proces. Bewijs in strijd met de privacyregelgeving wordt thans enkel van het bewijs uitgesloten bij ernstige inbreuk op de privacy. Dit geldt in Nederland en België zowel voor de civiele als de strafrechtelijke praktijk. Watermerken worden daarmee enkel van het bewijs uitgesloten wanneer de rechthebbende zijn processen zo inricht dat deze een ernstige schending opleveren van de privacy van de licentienemer. Daar zal in de regel niet snel sprake van zijn.

Dat watermerken in beginsel niet van het bewijs worden uitgesloten lijkt mij vanwege de beperkte schending van het privacyrecht een aanvaardbare uitkomst. Het is maatschappelijk onwenselijk dat mensen zich achter hun privacyrechten kunnen verschuilen om het gevolg van hun onrechtmatig handelen te ontlopen. Het omgekeerde lijkt mij evenzeer waar. Namelijk dat de rechthebbende geen direct voordeel mag trekken uit zijn onrechtmatig handelen. Wanneer uitsluiting van bewijs een te zwaar middel is en het niet sanctioneren van inbreuken op privacyrechten evenmin een optie is kan de rechter naar mijn mening het beste de onrechtmatige handelingen van partijen ‘verrekenen’ door in het civiele recht er met de toewijzing van de vordering expliciet rekening mee te houden. De rechter kan bijvoorbeeld andere sancties verbinden aan het schenden van privacyregels, zoals het toekennen van een schadevergoeding of het matigen van de toe te kennen schadevergoeding. Daarbij zou de rechter expliciet een verband moeten leggen tussen de schending en de sanctie die hij hieraan koppelt. In de lagere rechtspraak zijn hier inmiddels enkele voorbeelden van te vinden.

Uit het gebrek aan sanctionering in de huidige rechtspraak mag overigens niet worden afgeleid dat privacy geen enkele rol zou hoeven te spelen bij het ontwikkelen van watermerksystemen. Het structureel of beleidsmatig schenden van privacy kan de rechter ertoe brengen om het watermerk wel als bewijs uit te sluiten. Daarnaast moet niet worden onderschat dat, evenals bij de kopieerbeveiliging, schending van sociale en/of juridische normen tot maatschappelijk reacties kan leiden die de inzet van watermerken in de praktijk onmogelijk maken doordat consumenten de techniek niet langer accepteren. Voorlopig lijkt daar echter geen aanleiding toe.

6 Waarderen van watermerken

> 'The fact that an opinion has been widely held, is no evidence whatever that it is not utterly absurd; indeed in view of the silliness of the majority of mankind, a widely spread belief is more likely to be foolish than sensible.'[1]

6.1 Inleiding

In dit onderzoek is de effectiviteit van het watermerk onderzocht door de vraag centraal te stellen wanneer de rechter het watermerk binnen de grenzen die het bewijsrecht daaraan stelt kan aanvaarden als juridisch bewijsmiddel ter vaststelling van het feit dat het bestand aan de licentienemer toebehoort. Daartoe is in hoofdstuk 4 de plaats van het watermerk als bewijsmiddel in het bewijsrecht onderzocht. In hoofdstuk 5 kwam aan de orde in hoeverre het watermerk een toelaatbaar bewijsmiddel is. In dit hoofdstuk staat de laatste trede van de beoordeling centraal, namelijk de waardering van het watermerk door de rechter.

Het watermerk zal in de regel door de rechthebbende in de vorm van een onderzoeksverslag aan de wederpartijpartij en de rechter ter beschikking worden gesteld.[2] Wanneer de andere partij voldoende verweer heeft gevoerd is het aan de rechter om, eventueel met de hulp van een door hem benoemde deskundige, een oordeel te vormen over het watermerk.[3]

Over de wijze waarop de rechter tot zijn oordeel komt ten aanzien van het bewijs is niet veel bekend en dit is ook lastig te onderzoeken vanwege het individuele karakter van iedere zaak. Vanwege de relatieve nieuwheid van het watermerk als forensisch bewijsmiddel en het gebrek aan literatuur en jurisprudentie om watermerken als juridisch bewijsmiddel te kunnen beoordelen, is eerst onderzocht welke eisen aan vergelijkbaar forensisch bewijs worden gesteld en welke problemen zich in die domeinen voordoen bij de waardering van dat bewijs (par. 6.2). Daarna wordt er kort aandacht besteed aan de elementen die de rapportage van de rechthebbende zou moeten bevatten om het watermerk als betrouwbaar bewijsmiddel te kunnen beoordelen (par. 6.3). Hiermee wordt aan de rechthebbende, de licentienemer en de rechter duidelijk wat de minimale eisen zijn waaraan een watermerk als bewijsmiddel zou moeten voldoen om ervoor te zorgen dat de rechter het watermerk redelijkerwijs kan aanvaarden als juridisch bewijsmiddel ter vaststelling van het feit dat het bestand aan de licentienemer toebehoort.

Om tot een op waarheid berustende beslissing te komen is het echter van belang om, na de vaststelling dat de resultaten van het onderzoek naar watermerken betrouwbaar zijn, aandacht

[1] Bertrand Russell in Marriage and Morals, New York, Liveright, 1929.
[2] Voor zowel het Nederlandse als Belgische strafrecht geldt dat de rechthebbende het verslag aan het Openbaar Ministerie ter beschikking zal stellen die op haar beurt dit verslag aan de wederpartij geeft.
[3] In de regel geldt dit voor beide onderzochte landen zowel naar civiel als strafrecht. Zie voor de verschillen tussen het civiel en strafrecht hoofdstuk 4.

te hebben voor de valkuilen die er bestaan bij het komen tot een bewijsbeslissing op grond van de onderzoeksresultaten. De rechter zal immers waakzaam moeten zijn dat op zichzelf betrouwbare informatie ook tot een juiste bewijsbeslissing leidt. Een onjuiste interpretatie van de onderzoeksresultaten kan immers leiden tot misvattingen over de sterkte van watermerken als bewijs.[4] Evenals bij forensisch DNA-bewijs geldt bij watermerken dat statistiek een belangrijke rol speelt bij het bewijs.[5] Bij beide middelen wordt bewijs geleverd in de vorm van een berekening van de kans dat het spoor aan een bepaald persoon toebehoort. Het is aan de rechter om deze kansberekening te vertalen naar een oordeel over de schuld van de gedaagde of verdachte. Uit met name psychologische literatuur is bekend dat in deze vertaalslag bepaalde risico's liggen ten aanzien van het op de juiste wijze interpreteren van de gegevens. Deze risico's hangen samen met de wijze waarop mensen in het algemeen informatie verwerken en meer specifiek hoe zij omgaan met kansberekening of getallen in het algemeen. In paragraaf 6.4 zal om die reden worden onderzocht welke valkuilen de rechter bij het interpreteren van in beginsel betrouwbare watermerken moet proberen te vermijden om tot een oordeel te komen dat zoveel mogelijk overeenstemt met de wijze waarop het daadwerkelijk is gegaan. Dat het gebruik van statistiek niet zonder risico's is blijkt onder meer uit de Nederlandse strafrechtzaak Lucia de B. waarin een verdachte uiteindelijk ten onrechte veroordeeld was. Na een korte reconstructie van de zaak wordt ingegaan op de vraag welke juridische lessen ervoor watermerken getrokken kunnen worden uit deze zaak (par. 6.5). Het hoofdstuk wordt afgesloten met een samenvatting en conclusie (par. 6.6).

6.2 Waarderen van forensisch onderzoek: lessen uit ander forensisch bewijs

Bij gebrek aan wetgeving en jurisprudentie zal de rechter zijn oordeel over watermerken steeds baseren op de wijze waarop rechters en andere deskundigen in andere forensische disciplines zijn omgegaan met het beoordelen van forensisch bewijs.[6] Vanwege de relatieve nieuwheid van het watermerk als forensisch bewijsmiddel wordt in deze paragraaf eerst onderzocht welke eisen aan vergelijkbaar forensisch bewijs worden gesteld en welke problemen zich in die domeinen voordoen bij de waardering van dat bewijs.[7]

Voor het beoordelen van watermerken kan aansluiting worden gezocht bij het relatief nieuwe domein van digitaal forensisch bewijs.[8] Algemene eisen die aan digitaal forensisch onderzoek worden gesteld, spelen ook een rol bij forensisch onderzoek naar watermerken. Bijvoorbeeld de wijze waarop bewijs verzameld wordt en bewijs moet worden bewaard. Daarnaast is een

[4] In die zin houden de valkuilen ook een risico in voor de inzet van watermerken. Watermerken die op zichzelf betrouwbaar zijn kunnen door misvattingen alsnog hun waarde voor de rechthebbende verliezen.
[5] DNA is een afkorting voor Deoxyribonucleic Acid.
[6] Zie voor het gebrek aan een beoordelingskader vanuit de wet en jurisprudentie per paragraaf steeds de derde subparagraaf in hoofdstuk 4.
[7] Zie over de forensische tekorten o.m. de afscheidsrede Broeders in 2010 (Broeders 2010 A).
[8] Zie o.m. Pérez-Freire 2008, p. 1 en de verschillende congressen zoals het jaarlijkse SPIE-congres (Media Watermarking, Security, and Forensics). Ook de verwetenschappelijking van het forensisch werkveld in brede zin is betrekkelijk nieuw. Zie ook Broeders & Muller 2008 en het in 2012 begonnen multidisciplinaire NWO-programma forensic science dat ten doel heeft wetenschappelijke onderbouwing te bieden, risico te verminderen en de betrouwbaarheid van forensisch onderzoek te vergroten.

belangrijk element van het watermerk als bewijsmiddel, de zogenoemde kansberekening dat het spoor (gewatermerkte bestand) bij de vermeende dader (licentienemer) hoort. Dat element heeft het gemeen met forensisch DNA-onderzoek, dat als bewijs al veel meer en langer in de rechtszaal wordt gebruikt. Bijvoorbeeld in het strafrecht bij moord- of zedenzaken of in het civielrecht bij het vaststellen van vader- of moederschap.[9] DNA heeft zich daarbij reeds bewezen als een bewijsmiddel vanwege 'de grote overtuigingskracht welke aan een deugdelijk uitgevoerd DNA-onderzoek pleegt te worden toegekend'.[10] De geschiedenis van het gebruik van DNA als bewijs en de wijze waarop digitaal forensisch onderzoek tegenwoordig wordt gebruikt voor het leveren van bewijs kan belangrijke inzichten en aanknopingspunten bieden voor de wijze waarop de rechter het watermerk als bewijsmiddel tenminste zou moeten waarderen.

Watermerken en DNA hebben als bewijsmiddel een aantal overeenkomsten waardoor lessen uit dit domein van waarde kunnen zijn voor de waardering van het watermerk. Ten eerste was DNA als bewijs, evenals watermerken nu zijn, ooit een nieuw technisch bewijsmiddel waar veel van werd verwacht en dat nieuwe uitdagingen de rechtszaal binnenbracht.[11] Ten tweede is het bewijs in beide gevallen afkomstig uit de (forensische) praktijk waarin de opsporing van het materiaal en de toepassing van de wetenschappelijke kennis samenkomen. Ook worden beide bewijsmiddelen in de regel gepresenteerd in de vorm van een rapportage. Ten slotte wordt het resultaat uiteindelijk in beide gevallen weergegeven in de vorm van een kansberekening dat het spoor aan de vermeende dader toebehoort en waarbij voor de interpretatie ervan de hulp van één of meer deskundigen nodig kan zijn. Het belangrijkste verschil tussen DNA en watermerken als bewijsmiddel vormt de bron of de herkomst van de informatie. Een belangrijk onderscheid met DNA is dat de bron of het object van onderzoek (het bestand) van nature fragiel is.[12] In tegenstelling tot DNA-materiaal is het eenvoudig om de bron zelf – een digitaal bestand – te manipuleren waardoor het onderzoeksobject zelf al kritisch moet worden bekeken. Anders dan bij DNA-materiaal kan er gerede twijfel zijn over de betrouwbaarheid van de bron van het onderzoek.[13]

Op grond van de literatuurstudie en gesprekken met deskundigen zijn een aantal onderwerpen onderscheiden die in relatie tot het onderzoek naar watermerken als object van forensisch

[9] Zie o.m. HR 25 maart 2005, ECLI:NL:HR:2005:AT0412, JPF 2005/56 m.nt. P. Vlaardingerbroek (vaststellen vaderschap) en HR 18 januari 2013, ECLI:NL:HR:2013:BY0535 (vaststellen moederschap inzake vaststellen nationaliteit)

[10] HR 7 mei 1996, NJ 1996, 573, ov. 7.4; HR 8 december 2009, ECLI:NL:HR:2009:BI5746, ov. 2.6.

[11] Zie voor de relatieve nieuwheid en verwachtingen rondom watermerken par. 2.2.1. Zie voor de verwachtingen rondom DNA-bewijs o.m. Toom 2010 (diss.).

[12] U.S. Department of Justice, Office of Justice Programs National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement 2004, p. 1. http://nij.gov/nij/pubs-sum/199408.htm; https://www.ncjrs.gov/pdffiles1/nij/199408.pdf; ACPO, 'Good Practice Guide for Computer-Based Evidence' 2010, p. 6.

[13] Zowel bij DNA als bij een (computer)bestand kan het voorkomen dat er onvoldoende materiaal is om onderzoek op te verrichten of kan het spoor gemanipuleerd zijn. In het geval van DNA door bijv. ergens een haar van iemand anders achter te laten. Dat laat onverlet dat als er eenmaal voldoende DNA gevonden is, DNA als object van onderzoek altijd betrouwbaar is. Anders dan bij een bestand hoeft DNA zelf niet meer op manipulatie gecontroleerd te worden. In die zin is een digitaal bestand van nature meer fragiel dan DNA.

onderzoek en de verslaglegging van dat onderzoek van belang zijn voor het gebruik van watermerken in de rechtszaal.[14] Allereerst het forensisch onderzoek zelf. De aandacht voor forensische rapportages richt zich in de literatuur voornamelijk op twee aspecten: de kwaliteit van het onderzoek en de mate waarin juristen de rapportage begrijpen.[15] Daartoe wordt eerst aandacht besteed aan de kwaliteit van het onderzoek (par. 6.2.1) en de onderzoeker (par. 6.2.2). Vervolgens wordt gekeken naar een steeds terugkerend thema in de literatuur, namelijk de vertaalslag die gemaakt moet worden tussen juristen en andere deskundigen bij het beoordelen van het onderzoeksverslag dat als bewijsmiddel moet dienen (6.2.3). Tenslotte wordt aandacht besteed aan de vraag waaraan een goed onderzoeksrapport moet voldoen (par. 6.2.4). De paragraaf wordt afgesloten met een tussenconclusie (par. 6.2.5).

6.2.1 Kwaliteit van het onderzoek

De ontwikkelingen in het Nederlandse strafrecht naar aanleiding van verschillende strafrechtelijke dwalingen heeft in Nederland geleid tot extra aandacht voor de kwaliteit van onderzoek.[16] In de forensische literatuur is dan vanzelfsprekend aandacht voor de kwaliteit van het onderzoek.[17]

Voor digitaal forensisch onderzoek in het algemeen noch voor watermerken zijn er algemeen geldende richtlijnen opgesteld.[18] In Nederland bestaan voor forensisch onderzoek naar digitaal bewijs wel richtlijnen, maar deze hebben geen formele status.[19] De kwaliteit van het onderzoek wordt om die reden sterk bepaald door de onderzoeker en de organisatie waarvoor hij werkt.

[14] Zie voor de literatuur o.m. Broeders & Muller 2008. De geraadpleegde experts waren werkzaam bij het NFI, Ernst & Young, FOX-IT. Daarnaast, zij het op meer informele wijze, door middel van gesprekken met mensen in het veld op bijeenkomsten binnen het NWO-programma Forensic Science.

[15] Zie ook Taverne e.a. 2013, p. 9.

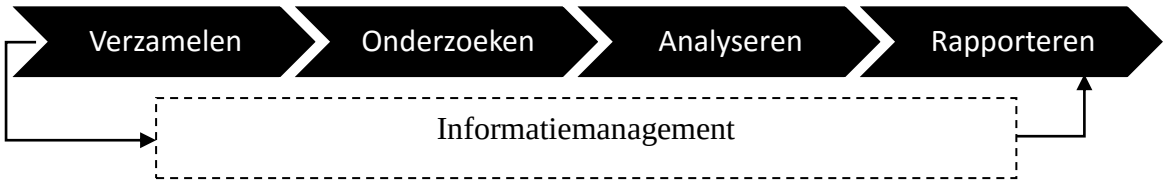
[16] HR 26 juni 2001, ECLI:NL:PHR:2001:AA9800, NJ 2001, 564, m. nt. Sch. (Herziening Puttense moordzaak II); HR 25 januari 2005 ECLI:NL:PHR:2005:AS1872 (Herziening Schiedammer Parkmoord II); HR 7 oktober 2008, ECLI:NL:HR:2008:BD4153, NJ 2009, 44 m. nt. P.A.M. Mevis (herziening Lucia de B.). Zie o.m. Bhoedjang 2008, p. 396; Koops 2010 e.a. p. 20. Omdat veel organisaties die deze onderzoeken verrichten zowel in het strafrecht als in het civiel recht optreden is er geen kwaliteitsverschil te verwachten tussen verslagen in het civiel en strafrecht.

[17] Zie specifiek voor digitaal forensisch onderzoek en forensische principes o.m. Bhoedjang 2008; Casey 2010.

[18] Zie o.m. Rb. Rotterdam (24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey) ov. 4.); Koops e.a. 2012, p. 50. Kessler (2010 (diss.), p. 12) geeft in zijn onderzoek naar digitaal bewijs in de Amerikaanse rechtspraak aan dat digitaal bewijs nog geen universeel geaccepteerde definities, fundamenteel onderzoek en ruim beschikbare literatuur kent.

[19] Zie ook Koops e.a. 2012, p. 50. Zie bijvoorbeeld de forensisch technische normen (FT-normen) die door het NFI zijn opgesteld en intern gelden voor het onderzoek op plaats delict en het vervoeren en overdragen van sporen. Deze voorschriften gelden dan ook niet als dwingende voorschriften waaraan het onderzoek aan bijvoorbeeld een computer dient te voldoen. Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey) ov. 4. in navolging van haar getuige-deskundige Bhoedjang. Voor zover mij bekend worden deze voorschriften door de rechter ook niet vereist bij het gebruik van dergelijke onderzoeken.

Om tot verantwoorde resultaten uit onderzoek te komen zijn in de literatuur in het domein van digitaal forensisch onderzoek verschillende modellen ontwikkeld.[20] Deze modellen bevatten verschillende fasen die doorlopen moeten worden om tot een verantwoord resultaat van het onderzoek te kunnen komen. Alle modellen bevatten fases van verzamelen (collection), onderzoeken (examination), analyseren (analysis), en rapporteren of presenteren (reporting or presentation).[21] Sommige modellen besteden daarnaast aandacht aan fases, zoals de voorbereiding en identificatie van de omvang van het probleem.[22]



Digitaal forensisch onderzoek in fasen

Nagenoeg alle modellen besteden aandacht aan het interne proces en daarmee aan de vraagstukken van kwaliteits- en informatiemanagement in brede zin. De juiste invulling en toepassing van deze modellen moet het mogelijk maken om een zogenoemde Chain of Custody te bewerkstelligen.[23] Een Chain of Custody kan dan worden omschreven als een ononderbroken spoor van verantwoording dat ertoe strekt zekerheid te bieden ten aanzien van de betrouwbaarheid van bepaalde data. Een dergelijk systeem van Chain of Custody heeft twee basiselementen. Ten eerste het bewijs dat data van een bepaalde bron afkomstig is en ten tweede een voor een audit vatbare dataverzameling in combinatie met een systeem dat in staat is een verband te leggen met het bewijs dat ieder product identificeert. Naast de Chain of Custody die ziet op de integriteit van het bewijs zelf, wordt er in de literatuur ook gewezen op het organiseren en presenteren van verschillende resultaten van zowel het fysieke als het digitale bewijs en het opstellen van een tijdlijn en in een keten van bewijs (Chain of Evidence). Deze keten van bewijs moet, bekeken vanuit een bepaalde volgorde, leiden tot het bewijs van bepaalde gebeurtenissen van een bepaald persoon of gedurende een bepaalde periode.

Om de verzamelde data uiteindelijk als bewijs te kunnen gebruiken is het dan ook van belang dat in alle fasen wordt vastgelegd welke handelingen zijn verricht en wat is aangetroffen.[24]

[20] Zie o.m. Kessler 2010 (diss.), p. 6; DFRWS 2001, p. 17; NIST 2004, p. 1; Kent e.a. 2006, p. 2-2. Voor een vergelijkbare indeling zie ook Jones & Valli 2009; Electronic Discovery Reference Model (EDRM.net). Zie ook (Nederlands strafrechtelijke) Aanwijzing technisch onderzoek/deskundigenonderzoek waarbij onderscheid wordt gemaakt tussen de eerste fase ofwel voorfase van het opsporingsonderzoek (dat is de fase van het verzamelen en veiligstellen én van het voorbereidend onderzoek aan sporen) en de fase van de interpretatie en analyse van het verkregen sporenmateriaal.
[21] Sommige modellen besteden daarnaast aandacht aan de fase van voorbereiding en identificatie van de omvang van het probleem of de vraag, alsmede aan managementvraagstukken, zoals archivering.
[22] Zie voor een overzicht tot 2008, Siti Selamat, Yusof & Sahib 2008, p. 163-169.
[23] Zie ook Casey 2011; Kessler 2010, p. 6.
[24] In veel gevallen zullen er ook logs worden bijgehouden.

Voor al deze stappen geldt dat duidelijk gemaakt moet kunnen worden waarom de gekozen stappen, het uiteindelijk gevolgde proces betrouwbaar maken. Dat kan in de praktijk bijvoorbeeld door het proces zo in te richten dat op basis van een bestaande methode kan worden aangetoond dat in de praktijk zich weinig problemen voordoen. Voor watermerken zal dat betekenen dat de rechthebbende in staat moet zijn een beschrijving te geven van het gehele model van authenticatie van de persoon tot het interpreteren van het watermerk. Hierbij spelen dan vragen een rol over de wijze waarop de techniek wordt ingezet en of en aan wie en hoe de detectiesoftware en sleutel ter beschikking zijn gesteld. Zo zal ook duidelijk moeten worden op welke wijze de sleutels en het algoritme van het watermerk zijn beveiligd.[25] In de praktijk blijft het een balans tussen werkbaarheid en veiligheid.[26]

Naast specifiek technische zaken is er in de literatuur ook aandacht voor organisatorische en beleidsmatige aspecten van onderzoek. Organisaties die zich bezighouden met (digitaal) forensisch onderzoek zullen gebruik (moeten) maken van beleid en procedures voor het uitvoeren van het onderzoek. Dat betekent dat zij niet alleen inzicht hebben in de keten van het bewijs van verzamelen van bewijsstukken tot presenteren en het bewaren van het onderzochte materiaal, maar ook in de wijze waarop de organisatie verder is ingericht, van de training van het personeel tot de beveiliging van het complex. Het antwoord op de vraag in hoeverre en op welke wijze deze fasen of keten is ingericht bepaalt in belangrijke mate de betrouwbaarheid van het onderzoek. Een zorgvuldig ingerichte keten biedt bovendien de mogelijkheid om de resultaten later te kunnen verantwoorden en te presenteren.

In het kader van kwaliteit wordt in de forensische literatuur continue aandacht gevraagd voor het ontwikkelen van standaarden en het verhogen van de kwaliteit van forensisch onderzoek door een uniform kwaliteitszorgsysteem, bijvoorbeeld door middel van accreditatie, zodat partijen eenvoudiger tot het selecteren van experts en onderzoek kunnen komen.[27] Koops e.a. constateren dat de meeste in Nederland actieve instituten een accreditatie hebben voor één of meer typen onderzoek en vormen van zelfregulering hanteren.[28] Hierbij kan worden gedacht aan het standaardiseren van (technische) processen, de wijze van samenwerking tussen de ketenpartners en het managen daarvan. Maar ook zelfregulering door certificering, interne audits en het organiseren van tegenspraak en reviews voordat resultaten gepresenteerd worden. Voor deze kwaliteitswaarborgen geldt dat zij allemaal bijdragen aan de betrouw-

[25] Bij de beveiliging kunnen grofweg drie zwakke plekken worden aangewezen: intern (personeel), waarbij vragen spelen als wie hebben er toegang e.d., inhoud (watermerk), hoe wordt het materiaal bewaard, hoe zijn de reacties op noodsituaties, e.d. en extern (systemen), waarbij vragen een rol spelen als wie komen er binnen en gaan naar buiten.

[26] In theorie kan van alles een ‘log’ worden bijgehouden. In het kader van beveiliging en computerpreformance is het echter in de praktijk niet wenselijk om alles bij te houden. Wat redelijk is wordt, evenals veel ander forensisch bewijs, veelal in een internationale context bepaald.

[27] Zie o.m. Koops 2010 e.a. p. 41; Muller 2008, p. 734, 736; Broeders 2003 (diss.), p. 444, waar Broeders er tevens terecht op wijst dat consensus mogelijk kan leiden tot een breed gedragen beslissing, maar dat die beslissing geen garantie is voor een juiste beslissing.

[28] Koops e.a. 2010, p. 55; Smithuis, Van Ruth & Wieles 2012. Zie voor accreditatie bijvoorbeeld de ISO-standaard 17025. ‘General requirements for the competence of testing and calibration laboratories’. Deze standaard is tegen betaling van CHF118 beschikbaar via www.iso.org.

baarheid van de resultaten maar ook geen garanties bieden. Een bekend voorbeeld is de gekraakte beveiligingscertificaten van Diginotar in 2011. Het bedrijf was gecertificeerd en daarnaast was er ook een audit uitgevoerd door een van de 'big four' accountantskantoren. Nader bezien had de audit zich echter alleen beperkt tot de managementkanten en niet gericht op de technische kant.[29] Het streven naar een betere kwaliteit is lovenswaardig, maar blijkt in de praktijk niet eenvoudig. Zo blijkt het niet eenvoudig om tot standaardisering en validering in digitaal forensisch onderzoek te komen.[30] Het valideren van onderzoeksprogrammatuur verloopt moeizaam.[31] Vaak is het testen arbeidsintensief en zijn de testresultaten slechts geldig voor een specifieke versie van bepaalde apparatuur of programma's. Omdat ook producenten geen gestandaardiseerde testresultaten bekend maken, blijft het lastig om onderzoeksmiddelen te valideren. Een ander aspect dat door deskundigen naar voren is gebracht, is dat veel aanbieders van zogenoemde closed source software een goede marketing voeren waardoor de bekendheid van het middel groter kan zijn dan de betrouwbaarheid ervan. Door de verscheidenheid aan middelen en de snelle ontwikkeling van software is het in de praktijk lastig om deze software gevalideerd te krijgen door bijvoorbeeld het National Institute of Standaards and Technology (NIST) in de Verenigde staten.[32] Voorlopig wordt voor het vaststellen van de betrouwbaarheid van methoden en applicaties die gebruikt zijn bij het zoeken en vaststellen van sporen gekeken naar het internationale forum.[33] Wat gebruiken andere onderzoekers en zijn er zaken bekend waarin deze applicaties door rechters zijn geaccepteerd of in ieder geval niet afgekeurd? In de praktijk blijft het maatwerk per (rechts)zaak en zal de rechter de toelaatbaarheid van de verschillende methodieken bepalen, al dan niet met de hulp van een deskundige.

Ondanks de wenselijkheid van standaardisering en validering zijn er ook voor watermerken geen standaarden ontwikkeld die de waardering vereenvoudigen.[34] Voor de vraag of de juiste watermerktechniek is ingezet kan gebruik worden gemaakt van ontwikkelde benchmarking-methoden.[35] De technische of zelfs wetenschappelijke standaard is echter lastig vast te stellen. In het verleden zijn er wel enkele werkgroepen bezig geweest, zoals in het kader van de Copy Protection Technical Working Group en Digital Audio-Visual Council (DAVIC).[36] De MovingPicture Experts Group (MPEG consortium) ontwikkelde als onderdeel van het MPEG 21 framework een standaard voor de evaluatie van 'persistent association technologies',

[29] Pels 2011, Trouw 6 september 2011. Zie ook het uiterste kritische rapport van Fox-IT over beveiliging van Diginotar http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html.
[30] Boddington, Hobbs & Mann 2008, p. 6.
[31] Bhoedjang 2008, p. 396. Dit is ook bevestigd in gesprekken met deskundigen.
[32] Dit instituut valideert en publiceert resultaten met betrekking tot apparatuur en programmatuur.
[33] Zoals blijkt uit gesprekken met verschillende digitaal forensisch experts.
[34] Zie Schellekens 2010. In de watermerkliteratuur wordt vooral het gebrek aan standaardisatie en validatie in de praktijk als een groot probleem ervaren. Dit belemmert niet alleen de ontwikkeling van watermerken in de praktijk, maar ook de verdere verspreiding daarvan in termen van gebruik. Hoewel het gebrek aan deze elementen de betrouwbaarheid van de watermerktechnieken in beginsel niet aantast levert het ook geen positieve bijdrage aan de perceptie van betrouwbaarheid.
[35]Zie o.m. Kutter & Petitcolas 2000; Macq, Dittman & Delp 2004; Marini e.a 2007; Kamiyae.a. 2010
[36]Zie o.m. Delaigle 2000, p. 2; Cox e.a. 2008, p. 47; Schellekens 2010, p. 161.

waaronder watermerk en fingerprinttechnieken.[37] Deze procedure vertoont gelijkenis met die van de aanschaf van maatwerksoftware, waarin naast functionele eisen ook best practices, testen en evaluaties zijn opgenomen. In de keten kan men gebruik maken van de hier genoemde best practice en voor de evaluatie verwijzen naar benchmarks, zoals Stirmark, Checkmark, Optimark, Openwatermark en WET (Watermark Evaluation Testbed).[38] Deze benchmarks blijven afhankelijk van de toepassing van de watermerksystemen en technieken. Om die reden wordt er ook in het MPEG 21 framework niet in detail ingegaan op de implementatie en evaluatie. Benchmarks van commerciële watermerkproducten zijn voor zover mij bekend op dit moment niet publiekelijk beschikbaar.[39] Cox e.a. geloven helemaal niet in een benchmarksysteem dat relevant kan zijn voor alle watermerksystemen en toepassingen.[40] In het MPEG framework is dan ook gekozen voor een best practice benadering. Een dergelijke benadering zegt in beginsel weinig over de implementatie en de deskundigheid waarmee de interpretatie plaatsvindt.

Zowel voor digitaal forensisch onderzoek in het algemeen als voor watermerken in het bijzonder zijn tot nu toe geen bruikbare standaarden ontwikkeld. Specifiek voor watermerken kan dan ook dezelfde conclusie worden getrokken als eerder ten aanzien van ander digitaal forensisch bewijs, namelijk dat de betrouwbaarheid van het bewijs vooral een kwestie zal zijn van specifiek onderzoek in individuele (rechts)zaken. Hoewel standaarden van belang zijn bij het accepteren van bepaalde bewijsmiddelen zullen uiteindelijk de uitspraken van een deskundige meer gewicht in de schaal leggen.[41] Hierdoor zullen partijen en de rechter zeker bij de eerste rechtszaken zijn aangewezen op bevindingen van experts en deskundigen.[42]

Samenvattend kan worden gesteld dat de resultaten uit het onderzoek(sverslag) geloofwaardig en betrouwbaar zijn wanneer kan worden aangetoond dat de resultaten zijn verkregen op basis van een model waarin de verschillende fasen van het onderzoek (verzamelen, onderzoeken, analyseren en rapporteren) zijn opgenomen en de uitvoering daarvan heeft plaatsgevonden binnen de algemeen geldende normen van het internationale forum.[43] Duidelijk is geworden dat er geen direct bruikbare standaard is voor digitaal forensisch onderzoek naar watermerken. Dat betekent in de praktijk dat bij de waardering van het watermerk als bewijsmiddel het onderzoeksverslag van de (partij-)expert en eventueel de rol van de door de rechter benoemde deskundige toeneemt. In dat kader is het van belang oog te hebben voor de kwaliteit van de onderzoeker.

[37] ISO/IEC TR 21000-11:2004 Information technology - Multimedia framework (MPEG-21), Part 11: Evaluation Tools for Persistent Association Technologies.
[38] Voor een overzicht zie verder Macq, Dittman & Delp 2004; Michiels & Macq 2006.
[39] TNO, Privacytoets HDIeF (Herkenning Digitale Informatie en Fingerprinting; NCTb), 2011-12, 2010, p. 37.
[40] Cox e.a. 2008, p. 48.
[41] Mason (2012, p. 86) constateerde dit reeds voor common law landen.
[42] Gesprekken met I. Lagendijk (TU Delft). Zie ook Schellekens 2010.
[43] Dit staat los van de vraag of rechters dit ook daadwerkelijk lezen. Onderzoek van Taverne e.a. 2013 wees uit dat rechters in een onderzoek naar het lezen en begrijpen van DNA-rapportages informatie hebben gemist over de wijze waarop het DNA-onderzoek is uitgevoerd.

6.2.2 Kwaliteit van de onderzoeker

De kwaliteit van het onderzoek en het verslag daarvan worden voor een belangrijk deel bepaald door kwaliteiten (kennis en ervaring) van de expert of deskundige die deze taken verricht.[44] De door partijen ingebrachte experts evenals de door de rechter aangewezen deskundige spelen een belangrijke rol in de informatievoorziening aan de in beginsel niet deskundige partijen en rechter. Partijen en de rechter zijn voor een betrouwbare informatievoorziening ten aanzien van forensisch bewijs veelal afhankelijk van de mate waarin de aangewezen persoon zijn deskundigheid en onafhankelijk heeft kunnen inzetten. Tegelijk wordt er in de literatuur op gewezen dat de persoon van de deskundige een zwakke schakel kan vormen aan het bijdragen van een oplossing in een juridische kwestie.[45]

Uit verschillende onderzoeken lijkt naar voren te komen dat (straf)rechters door tijdsdruk vaak de moeite niet nemen om zich in een complex deskundigenrapport te verdiepen en ze daarom vrijwel volledig vertrouwen op de expertise van de deskundige.[46] Eenzelfde situatie is voorstelbaar ten aanzien van de situatie in het civiel recht.[47] Enerzijds zijn er signalen dat Nederlandse rechters in civiele zaken experts van partijen en hun onderzoeken wantrouwen.[48] Anderzijds is het zeker niet onvoorstelbaar (maar niet onderzocht) dat ook Nederlandse civiele rechters door tijdsdruk vaak de moeite niet nemen om zich in een complex deskundigenrapport te verdiepen en ze daarom vrijwel volledig vertrouwen op de expertise van een expert of deskundige. De door de rechter benoemde deskundige speelt daarbij in Nederland de belangrijkste rol omdat de Nederlandse civiel rechter vanwege de hoge motiveringseisen ten aanzien van zijn vonnis nauwelijks van zijn verslag kan afwijken.[49] In dit laatste geval wordt dat bewijsmiddel dan ook snel van doorslaggevende betekenis, omdat de rechter inhoudelijk niet anders kan dan vertrouwen op het oordeel van de door hem aangestelde deskundige.

De markt voor forensisch onderzoek is in de civiele praktijk in beginsel een open markt. Dat geldt ook voor het strafrecht. Niettemin heeft het Nederlands Forensisch Instituut (NFI) daarin een bijzondere positie vanwege de financieringsstructuur van forensisch onderzoek en de neiging van de politie en het Openbaar Ministerie (hierna: OM) aan te kloppen op het oude

[44] In dit hoofdstuk wordt met de term deskundige diegene bedoeld die door de rechter is aangesteld als deskundige. De term expert verwijst naar degene die door een partij als (partij-)deskundige wordt ingezet.
[45] Zie o.m. Giard 2014 en eerder Broeder 2003, p. 413. Giard wijst in dit artikel op de zwakke plekken bij de inzet van een niet partij gebonden deskundigen. En vraagt zich af welke maatregelen effectief en mogelijk zijn. Formele regels en certificering leiden volgens Giard tot meer discipline, de inhoudelijke bemoeienis zou van beroepsorganisaties moeten komen. Maar de daadwerkelijke controle zou naast van voornoemde instanties, ook van rechters en advocaten moeten komen omdat zij verantwoordelijk zijn voor de context waarbinnen hij opereert en de deskundige kunnen dwingen om niet te vrijblijvend te opereren.
[46] Taverne e.a 2013, p. 42 en de daar aangehaalde onderzoeken.
[47] In alle landen en rechtsgebieden wordt in de literatuur melding gemaakt van de hoge werkdruk van rechters. Zie voor het Belgische civiel recht bijvoorbeeld Allemeersch 2007 (diss).
[48] Zie o.m. Visser 2008, p. 1922.
[49] Zie hoofdstuk telkens de derde subparagraaf (4.2.3.2, 4.3.3.2, etc). Dat is anders in België waar de rechter ook geheel vrij is in de waardering van de inbreng van de door hem benoemde deskundige.

vertrouwde adres.[50] Voor beide markten geldt dat de externe controle op de kwaliteit veelal ontbreekt.[51] De overtuiging van forensisch onderzoekers is dat je het vak vooral leert door ervaring. De rechter en partijen moeten om die reden waakzaam zijn voor het gebruik van de juiste experts en deskundigen.[52] Er wordt dan ook wel gepleit voor een systeem van toelating en beoordeling voordat een expert als forensisch expert kan worden aangezocht en als deskundige in de rechtszaal kan worden gehoord.[53] Ook de rol als onafhankelijk expert wordt daarbij genoemd in relatie tot zijn opdrachtgevers (partijen of OM).

Het staat partijen in zowel het civiel als strafrecht vrij om een expert aan te stellen die voor hen onderzoek verricht. De wijze van waarderen van het watermerk hangt zoals gezegd samen met de kwaliteit van de onderzoeker. Om die reden zou bij het aanstellen van een dergelijke onderzoeker houvast kunnen worden gevonden in de eisen die worden gesteld aan een door de rechter gevraagd deskundigenbericht.[54]

Dat betekent dat ook van een (partij-)expert gevraagd kan worden dat hij op grond van zijn bijzondere kennis de partijen en de rechter zo correct mogelijk voorlicht over de (in het rapport) aan hem gestelde vragen. Aan de door de rechter benoemde deskundige zijn verder kort gezegd de eisen gesteld dat hij zijn opdracht deskundig, onpartijdig en naar beste weten verricht.[55] Een belangrijk verschil met het deskundigenbericht is dat de rechter een onafhankelijke deskundige kan aanwijzen. De partij-expert zal de schijn in ieder geval altijd tegen hebben.[56] Hij zal in zijn rapportage blijk moeten geven van zijn onpartijdigheid door een verslag te schrijven waarin hij de rechter op grond van zijn eigen deskundigheid overtuigt dat hij tot een onafhankelijk oordeel is gekomen. Bijvoorbeeld door ook aandacht te besteden aan verklaringen die niet het primaire belang van de rechthebbende dienen. De expert op het gebied van watermerken zal bij een gebrek aan een specifieke professionele standaard voor digitaal watermerkexperts moeten terugvallen op de standaarden die gelden voor deskundigen in het domein van digitaal forensisch deskundige of deskundigen in het algemeen.

[50] Zie o.m. Koops 2010, p. 8 en verder uitgebreid in de verslaglegging van het onderzoek. Het NFI heeft een uitzonderlijke positie vanwege de bulkfinanciering aan het NFI uit de begroting van het ministerie van Justitie.
[51] Zie voor de markt van forensisch onderzoek en de kwaliteit daarvan o.m. Koops e.a. 2010 en Baarsma & Van Buiren 2010. Grote spelers op de markt zijn wel bezig meer controle in te bouwen.
[52] KNAW (o.m. Prins), 1e forensische symposium 2012, o.m. dhr. Groeneveld Rijnmond politie.
[53] Zie o.m. Muller 2008, p. 734. Met de invoering van de Wet deskundigen in strafzaken (Stcrt. 2009, 33; nr. 18632) is hiermee een begin gemaakt. Zie verder het Besluit register deskundige in strafzaken (Stcrt. 2009, 330) en de aanwijzing technisch opsporingsonderzoek/deskundigenonderzoek (Stcrt. 2013, 13962) (www.nrgd.nl). Voor meer beschouwingen over het de wet en het register verwijs ik o.m. naar het WODC-rapport van Keulen e.a. 2010; Nijboer 2011, p. 194. Zie voor opties tot vernieuwing van deskundigen in civiele zaken o.m. in vergelijking met België Krans & Santing-Wubs 2012.
[54] De grondslag van het door de rechter gevraagde deskundigenbericht kan worden gevonden in de waarheidsvinding en kan om die reden ook uitgangspunt zijn voor de waardering van een rapport van een niet door de rechter benoemde expert. Zie ook De Hek 2013, p. 110 ten aanzien van de betekenis van accountantsrapporten in de civiele procedure. Vgl. De Bock 2011, p. 289 en De Groot 2008 (diss.), p. 2. Zie ook hoofdstuk 4.
[55] Zie verder hoofdstuk 4.
[56] Zie ook het onderzoek van Visser 2008.

Watermerken vormen een specifiek domein dat vanuit meerdere disciplines wordt bestudeerd. Mede vanwege de verschillende onderwerpen die bij watermerken samenkomen kan het lastig zijn om te beoordelen wie deskundig is.[57] Iemand die een aantal artikelen gepubliceerd heeft over bijvoorbeeld zogenaamde collusion attacks bij watermerken met een traitor tracingsdoel, hoeft nog geen expert te zijn over het brede domein van watermerken.[58] Het is zowel voor partijen als voor de rechter bij het benoemen van een deskundige van groot belang dat deze deskundigheid bezit op het domein of domeinen waarover vragen worden gesteld, en waarin vragen kunnen worden verwacht.[59]

Voor zowel het opstellen als het latere beoordelen van het gepresenteerde onderzoek naar watermerken heeft het de voorkeur om iemand als expert of deskundige te benoemen die zowel kennis als ervaring heeft met watermerken en bij voorkeur met digitaal forensisch onderzoek.[60] De keuze voor een gerechtelijk deskundige hangt af van de door de rechter gestelde vraag. In het algemeen heeft het de voorkeur om iemand als deskundige aan te wijzen die ervaring heeft met (forensische) watermerken, omdat voor het beoordelen van een watermerk niet alleen wetenschappelijke kennis van belang is maar ook ervaring met watermerken in de praktijk een rol kan spelen bij de inschatting van de waarschijnlijkheid in het specifieke geval. Een statisticus vragen als deskundige om de kansberekeningen in dit proces te controleren lijkt mij weinig zinvol. Mede omdat het de taak is van de deskundige om de methodiek te bepalen per casus en algemeenheden van de wetenschap in een individueel geval niet altijd leiden tot resultaten die ook voor watermerken van belang zijn. Voor externe en onafhankelijke experts kan in Nederland worden gedacht aan de opgebouwde expertise bij de TU Delft en TU Eindhoven. En in België onder meer aan de Vrije Universiteit Brussel (VUB) of de Université Catholique de Louvain (UCL).[61]

Het belang van forensische kennis en ervaring van de benoemde experts en deskundigen is met name in die gevallen van belang waarin hen gevraagd wordt een uitspraak te doen over de mate van betrouwbaarheid in een bijzonder geval. Zo kan hij uitspraken doen over wat de gebruikelijke gang van zaken is en in welke situaties hiervan kan worden afgeweken zonder dat het direct de betrouwbaarheid aantast. Zo verklaarde de getuige-deskundige in de e-donkeyzaak waarin inbreuk op het auteursrecht centraal stond, dat het met het oog op het veiligstellen van het materiaal op de harde schijf gebruikelijk is dat bij digitaal onderzoek aan computers een back-up kopie van de harde schijf wordt gemaakt. Maar dat uitzonderingssituaties zich kunnen voordoen waarin hiervan kan worden afgeweken,

[57] Zie par. 2.2.1.
[58] Zie ook par. 6.5. over het benoemen van deskundigen (ten derde).
[59] Zie ook de zaak Lucia de B. (par. 6.5) waarin een jurist zonder bijzondere statistische expertise werd gevraagd om zich als deskundige uit te spreken over statische modellen.
[60] Voor externe en onafhankelijke experts kan in Nederland worden gedacht aan de opgebouwde expertise bij de TU Delft (Multimedia Signal Processing Group). En in Belgiëaan de VrijeUniversiteit Brussel (VUB; Department of Electronics and Information Processing (ETRO)) of de Université catholique de Louvain (UCL; Laboratoire de Télécommunications et Télédétection (TELE)).
[61]Vrije Universiteit Brussel (VUB), Department of Electronics and Information Processing (ETRO); Université Catholique de Louvain (UCL), Laboratoire de Télécommunications et Télédétection (TELE)

bijvoorbeeld wanneer de computer bij aantreffen aanstaat. In dit geval achtte hij 'live' onderzoek ter plaatse op de computer niet ongebruikelijk en zijn de verrichtte handelingen op de computer van verdachte niet ongebruikelijk.[62]

6.2.3 Vertaalslag tussen juristen en andere deskundigen

Ten aanzien van het waarderen van DNA-bewijs is er in de literatuur ook gewezen op de 'kloof' tussen juristen en andere deskundigen.[63] Er wordt in die zin veelal gesproken van twee werelden waarbij de alfa de bèta niet zou begrijpen.[64]

Zowel de kennisskloof als het gebrek aan communicatie in de rapportages en op de zitting zijn daarbij voortdurend punten van aandacht. Zoals De Knijff (2004) de kennisskloof in zijn oratie samenvatte: 'Vrijwel alle Nederlandse strafrechtadvocaten tonen bedroevend weinig belangstelling voor de complexiteit van forensisch DNA-onderzoek, en de meeste rechters snappen er volgens mij nog minder van en geloven de getuigenissen van de deskundigen klakkeloos.'[65] Onderzoek van Taverne e.a. (2013) laat zien dat de scherpe randen van deze observatie eraf zijn, maar dat de boodschap ervan nog steeds actueel is. Om een vertaalslag te kunnen maken tussen juristen en andere deskundigen is dan ook veelvuldig gepleit voor meer opleiding en voorlichting zowel voor juristen als voor experts om een brug naar elkaars wereld te slaan.[66] Vanuit de rechterlijke macht en vanuit deskundigen is hier dan ook steeds meer aandacht voor in allerlei opleidingen.[67] De eerder genoemde werkdruk en de angst van rechters om 'vertalingsfouten' te maken dragen echter niet bij aan het dichten van de kloof.[68] Een proef waarbij strafrechters forensische ondersteuning kregen bij het beoordelen van technisch bewijs lijkt succesvol genoeg om het project uit te breiden.[69]

---

[62] Rb. Rotterdam 24-07-2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey) ov. 4.

[63] Crombag 2000, p. 1663; Nijboer 2004; De Knijff 2004, 2006; Muller 2008, p. 736. Ook tijdens de KNAW-bijeenkomst 'Bèta in crime. Wetenschappelijk bewijs in rechtszaken', 11 juni 2012 kwam dit punt weer naar voren. Voor een beschrijving van de kloof tussen juristen en wetenschappers uit andere disciplines, zie: Broeders 2002, 2005; Crombag 2000; De Knijff 2004, 2006; Nijboer 2004. Ronald Prins (Fox-IT) vraagt (op de KNAW bijeenkomst 'Bèta in crime.' als deskundige aandacht voor het gevoel van de deskundige. Juristen die tijdens deze bijeenkomst reageren geven aan daar in de juridische praktijk (terecht) weinig mee te kunnen.

[64] Zie o.m. Broeders 2010 A, p. 5.

[65] De Knijff 2004, p. 48; Taverne e.a. 2013.

[66] Zie o.m. conclusie van het Rapport Posthumus (2005); Muller 2008, p. 738. Zie ook de afscheidsrede van Broeder 2010, p. 6.

[67] Al dan niet verplicht in het kader van registers. Volgens Broeders (2010, p. 6) moeten (strafrecht-)juristen beter toegerust worden op de confrontatie met de natuurwetenschap door te beschikken over elementaire kennis van de wetenschappelijke methode, de werking en de beperkingen van het cognitieve systeem, de besliskunde, de Bayesiaanse en de traditionele, frequentistischetoetsstatistiek, en de mogelijkheden en de beperkingen van veelvuldig toegepaste vormen van forensische expertise en de binnen die verschillende disciplines heersende rapportagecultuur. Zie in Nederland bijvoorbeeld het trainingsaanbod van Fox-IT en onderzoek in de Verenigde Staten naar het trainen van rechters (Kessler 2010). Sommige producenten bieden cursussen en certificering aan voor de kennis en het gebruik van hun eigen producten.

[68] Zie Taverne e.a. 2013, p. 42. 'Rechters en officieren van justitie daarentegen nemen, zoals eerder toegelicht, nog al eens een deskundigenconclusie één-op-één over om te voorkomen dat er 'vertalingsfouten' worden gemaakt. Zij hoeven dus minder uit te leggen. Het moeten uitleggen van een ingewikkeld probleem kan tot een diepere vorm van begrijpen van dit probleem leiden. Aangezien rechters niet gedwongen worden om uit te leggen, missen zij wellicht een stimulans om tot deze diepere vorm van begrijpen over te gaan.'

[69] http://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Forensische-ondersteuning-helpt-strafrechters.aspx

Prins ziet voor digitaal forensisch onderzoek echter weinig in het beter opleiden van rechters, omdat het verschil in het licht van de ontwikkelingen (te) groot blijft en daardoor te weinig bijdraagt aan een juiste vaststelling.[70] Op een KNAW-symposium over forensisch bewijs pleitte Prins voor het organiseren van veel meer discussie tijdens een zitting.[71] De deskundige blijft naar zijn mening nu te veel op een (zuivere) afstand, terwijl hij veel meer in de zaak zou moeten zitten.[72] Enkele rechters gaven op hetzelfde symposium aan dat ook zij de behoefte voelen om met deskundigen in discussie te gaan op de zitting om zaken duidelijker te krijgen.[73] Rechters gaven voor het civiel recht daarentegen wel aan dat het niet altijd mogelijk is omdat de wil van partijen een belangrijke plaats inneemt. Daarnaast gaven met name veel juristen aan dat de deskundige niet op de stoel van de rechter moet komen te zitten en dat de discussie vooral in de rechtszaal plaats moet vinden zodat ook partijen zich erover uit kunnen laten. Bij Taverne e.a. was de indruk ontstaan dat er geen duidelijke afspraken bestaan over de vraag hoe ver een DNA-deskundige mag gaan in het interpreteren van aan hem of haar voorgelegde DNA-onderzoekvragen en wanneer het noodzakelijk is om de opdrachtgever nadere informatie te vragen. Zij deden dan ook de aanbeveling om hier meer duidelijkheid in te scheppen.[74] Rechters zouden deze discussie naar mijn mening zeker op een zitting moeten voeren. In het civiel recht, waar het gebruik van het watermerk het meest voor de hand ligt, zou de rechter in het kader van de waarheidsvinding deze ruimte kunnen nemen. Met name in zaken waarin het watermerk voor het eerst wordt gebruikt. Op die manier kan bescherming worden geboden tegen de inzet van het watermerk als strategisch bewijsmiddel en kan ook de literatuur verder worden verrijkt.

Uit gesprekken met experts uit het veld blijkt tot slot dat er naast opleidingen ook een toenemende vraag is naar contra-expertise.[75] Zowel door de rechter die nadere vragen wenst te stellen als door partijen die graag vooraf een beter beeld willen krijgen over het door de wederpartij opgestelde rapport en wat dit betekent voor hun cliënt. Onderzoekers en deskundigen staan in beginsel positief tegenover een contra-expertise die uitgevoerd is door een deskundige partij. Als belangrijkste reden geven zij dat het iedereen scherp houdt en de

(2013).

[70] Prins (FOX-IT) in zijn presentatie tijdens de KNAW-bijeenkomst 'Bèta in crime. Wetenschappelijk bewijs in rechtszaken', 11 juni 2012.

[71] Zie ook Taverne e.a. 2013, p. 43 'In feite vragen lezers hiermee aan de deskundige om een stapje verder te zetten richting de juridische/politiepraktijk en een begin te maken met de overbrugging van de kloof tussen het laboratorium en de werkvloer van rechter, officier van justitie en rechercheur. Hoe groot deze stap kan zijn zonder dat de deskundige op de stoel van de rechter gaat zitten, vergt nader onderzoek.'

[72] Ook tijdens de KNAW-bijeenkomst 'Bèta in crime. Wetenschappelijk bewijs in rechtszaken', 11 juni 2012 kwam dit punt weer naar voren. Prins (Fox-IT) hanteerde als stelling voor de discussie dan ook dat de rechter meer leert van een gesprek met de deskundige bij het koffiezetapparaat dan van het rapport. Zie in dat licht ook het plan van D66 om in complexe rechtszaken vaker deskundigen op te nemen in de zittingskamer. http://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Raad-voor-de-rechtspraak-%E2%80%98Deskundigen-als-rechter-verkenning-waard%E2%80%99.aspx (laatste geraadpleegd op 31-12-2013).

[73] KNAW bijeenkomst 'Bèta in crime. Wetenschappelijk bewijs in rechtszaken'.

[74] Taverne e.a. 2013, p. 98.

[75] De meeste deskundigen refereren hier naar zaken in het strafrecht, maar ook (zij het in mindere mate) naar het civiel recht in zaken waar fraude een rol speelt.

kans op een tunnelvisie vermindert, zowel bij de juristen als de experts en deskundigen.[76] De kans op betrouwbare onderzoeksresultaten neemt toe wanneer de deskundige gespecialiseerd is in IT en bij voorkeur ervaring heeft met forensisch onderzoek.

Zowel de toenemende vraag naar opleidingen als de verplichte scholing voor gerechtelijk deskundigen is een stap in de goede richting. Ook een toenemende vraag naar contra-expertise duidt erop dat partijen het belang van forensisch onderzoek inzien. De basis voor een betere beoordeling van forensisch bewijs lijkt hiermee gelegd. De volgende stap is het verbeteren van de vertaalslag tussen juristen en andere deskundigen. Taverne e.a. lieten immers zien dat daar nog veel te winnen is. Inmiddels wordt ook op dat terrein nieuw onderzoek verricht en meer gericht gezocht naar oplossingen. De multidisciplinaire aanpak van die projecten maakt echter ook duidelijk dat de rechter en partijen zich niet voor een eenvoudige opdracht gesteld zien wanneer zij de waarde van forensisch bewijs moeten bepalen. Het feit dat het niet eenvoudig is brengt tegelijk risico's met zich mee ten aanzien van de waarheidsvinding. In hoeverre dat daadwerkelijk een probleem vormt voor de procesdeelnemers zal in de praktijk vooral afhangen van de uitslag van het proces en in hoeverre die overeenkomt met de werkelijke toedracht.

6.2.4 Rapporteren over forensisch onderzoek

Aan het verslag van de (partij-)expert en de deskundige worden in de forensische literatuur dezelfde eisen gesteld. In beide gevallen dient het verslag coherent te zijn, dat wil zeggen dat het geen innerlijke tegenstrijdigheden bevat (intern consistent) en begrijpelijk is. Voor beide verslagen geldt dan ook dat naarmate het verslag meer aan deze vereisten voldoet, de bewijskracht ervan zal toenemen. Behoudens deze algemene eisen worden er in de literatuur geen nadere eisen gesteld aan vormgeving van het verslag.[77]

Ten aanzien van de rapportage is er in de forensische literatuur, behalve voor de kwaliteit van het onderzoek, de laatste 10 jaar ook aandacht voor de wijze waarop de resultaten van het onderzoek worden overgebracht door de deskundige aan de rechter.[78] Onder meer Knijff merkt in 2004 ten aanzien van DNA-rapportages op dat deze moeilijk te lezen zijn voor juristen en dat de complexiteit van de analysemogelijkheden in de toekomst ook in meer complexe rapporten zal resulteren.[79] De aandacht voor de mate waarin juristen de DNA-rapportages daadwerkelijk begrijpen blijkt tien jaar later nog steeds actueel.[80] Onderzoek in 2009 en 2013 wijst uit dat zelfs juristen die aangaven de rapporten te begrijpen, vaak niet in staat waren op een juiste wijze de conclusie van het rapport te beschrijven.[81]

[76] Zie Bhoedjang 2008, p. 397. Alle gesprekspartners bevestigen dit beeld.
[77] Zie voor een model voor een deskundigenbericht: rechtspraak.nl.
[78] Zie o.m. Taverne e.a. 2013, p. 9 en de daar aangehaalde literatuur.
[79] Knijff 2004, p. 48; Van Koppen 2004.
[80] Zie ook Meulenbroek 2011.
[81] Raat, Heijnen & Malsch 2009, p. 157-162.; Taverne 2013 e.a., p. 41. In forensische literatuur wordt dit probleem ook onderkend en wordt gezocht naar oplossingen. Zie o.m. het onderzoek van Taverne e.a. 2013 naar het begrijpelijk maken van DNA-rapporten.

Het rapport moet dan ook in begrijpelijke taal geschreven worden in relatie tot de doelgroep. De expert of deskundige zal bij het rapporteren dan ook niet alleen aandacht moeten besteden aan het beschrijven van de mogelijke conclusies die in het algemeen mogelijk zijn maar ook wat de onderlinge verhouding is. Om die reden moeten alle gedocumenteerde stappen en statistische modellen wel beschikbaar zijn maar niet altijd volledig in het rapport worden opgenomen. Op die manier kan de rapportage beperkt worden in omvang, maar wel compleet en accuraat zijn. Daarnaast kan gedacht worden aan de wijze waarop de deskundige zijn bevindingen formuleert. De deskundige mag bijvoorbeeld zijn bevindingen niet op een wijze presenteren waarvan bekend is dat zij valkuilen, zoals prosecutor's of defence attorney's fallacy, oproept.[82] Wanneer het resultaat van onderzoek een kansberekening is, zoals bij DNA en watermerken, dan zal de rapportage niet alleen iets moeten zeggen over de kans, maar ook waar de kans iets over zegt en wat het spectrum daarvan is. De deskundige zal er daarbij rekening mee moeten houden dat juristen liever een verklaring in woorden krijgen dan een in cijfers.[83]

Dat geldt evenzeer voor het gebruik van afbeeldingen. Ook deze kunnen lezers afleiden van de specifieke inhoud in de rapportage.[84] Hetzelfde geldt voor het gebruik van bepaalde woorden of het presenteren van kwantitatieve gegevens in een formaat waarvan bekend is dat het de interpretatie in een bepaalde richting stuurt.[85] Bhoedjang wijst in het kader van de rapportage ook op de correcte formulering die veelal de onzekerheid weergeeft.[86] Zo is het weergeven van het ontstaan van een spoor voor zowel de lezer als schrijver eenvoudiger in een formulering als ‘Het bestand Factuur.doc is een Word-document dat op januari 2005 om 10.08 uur voor het laatst is gewijzigd.’ dan een formulering die met minder zekerheid gaat gepaard maar wel correcter is: ‘Het bestand Factuur.doc heeft het formaat van documenten zoals tekstverwerker Microsoft Word die produceert. Het document kan met die tekstverwerker ingelezen worden. Volgens informatie opgeslagen in het bestandssysteem is het document voor het laatste gewijzigd op 4 januari 2005 om 10.08 Nederlandse tijd.’ Een expert of deskundige zal in de regel ook niet met zekerheid kunnen vaststellen of bijvoorbeeld een document op een bepaalde dag is geprint, omdat de computertijd onjuist kan zijn maar ook omdat andere verklaringen van een spoor onduidelijk of niet bekend zijn. Het enige dat de expert of deskundige kan verklaren is dat, gegeven de handeling, hij door middel van testen in een laboratorium de aard van een spoor wel kan voorspellen. De deskundige ziet enkel een spoor en niet de handeling die is verricht. De handeling kan immers ook gebaseerd zijn op een foutieve invoer of een print die niet uit de printer is gekomen. Anders gezegd de lezer zal extra aandacht moeten hebben voor rapportages waarin de conclusies zonder enige

[82] Daarbij kan gedacht worden aan valkuilen zoals de conformation bias. Zie daarvoor par. 6.4.2
[83] Het NFI rapporteert om die reden tegenwoordig ook in termen van waarschijnlijkheid.
[84] Zie daarvoor o.m. Klaming 2010, p. 129.
[85] Broeders 2003 (diss.), p. 445. Bij woordgebruik kan gedacht worden aan het verschil tussen een rode vlek en bloed of een persoon en een dader.
[86]Bhoedjang 2008, p. 394.

twijfel of beperking in het onderzoek tot stand zijn gekomen. Absoluut bewijs bestaat immers niet.[87]

Bij de waardering van rapporten is het derhalve van belang om goed voor ogen te houden dat de conclusie en argumenten gebaseerd zijn op onderzoek dat is uitgevoerd volgens betrouwbare methoden en technieken. De rechter zal namelijk moeten beoordelen of de juiste methode of techniek is gebruikt en of deze methode of techniek ook juist is toegepast of uitgevoerd. Het lijkt geen twijfel dat de rechter daarvoor de hulp nodig heeft van een deskundige.

Opgemerkt moet worden dat het aanvallen van een rapportage door een expert altijd mogelijk is langs de lijn van de gehanteerde methodiek, de gebruikte vraagstelling of de wijze van berekening. In het proces zal, eventueel met behulp van deskundigen, duidelijk moeten worden wat de waarde is van de gehanteerde argumenten. Een verkeerde vraagstelling leidt immers niet per definitie tot een verkeerde uitkomst en een discussie over de methodiek maakt een onderzoek ook niet geheel onbetrouwbaar of de uitkomsten daarvan onjuist.

6.2.5 Tussenconclusie

Om zicht te krijgen op de beoordeling en verwachtingen van nieuwe technologieën en digitale watermerken in het bijzonder is in deze paragraaf gekeken naar de wijze waarop ander forensisch onderzoek als bewijs in de rechtszaal is en wordt gebruikt. Daarvoor zijn op basis van literatuur en gesprekken met deskundigen vier onderwerpen geselecteerd die ook voor de beoordeling van watermerken van belang kunnen zijn.

Ten eerste de kwaliteit van het onderzoek. Noch voor digitaal onderzoek in het algemeen noch voor watermerken gelden (nog) algemeen geldende richtlijnen. De kwaliteit van het onderzoek wordt om die reden sterk bepaald door de onderzoeker en de organisatie waarvoor hij werkt. Zowel ten aanzien van digitaal onderzoek als voor watermerken zelf bestaat er in de literatuur een behoefte aan standaardisering om het onderzoek meer vergelijkbaar en betrouwbaar te maken. In de praktijk blijkt het echter lastig om tot standaarden en validering van methoden te komen. Het internationale forum bepaalt voorlopig wat gangbaar is. Vanwege deze onduidelijkheid en de snelle ontwikkelingen binnen het domein van ICT zal er zeker bij de eerste rechtszaken behoefte zijn aan experts en/of deskundigen om duidelijk te maken of het onderzoek en de gebruikte methode aanvaardbaar zijn. De vraag wie deskundig is wordt daarmee van groot belang.

Ten tweede wordt er aandacht gevraagd voor de vraag wie als deskundige moet worden gevraagd. In tegenstelling tot door de rechter benoemde deskundigen bestaan er geen regels voor partij-experts. Vanwege de bewijskracht lijkt het de meest logische weg om voor de

[87] Zie ook Broeders in een interview met Bionieuws, editie: 19, 26 november 2004. http://www.bionieuws.nl/artikel.php?id=1660&print=1

eisen voor deze groep aansluiting te zoeken bij de eisen die aan een door de rechter benoemde deskundige worden gesteld. Dat betekent dat hij kort gezegd zijn opdracht deskundig, onpartijdig en naar beste weten moet verrichten.[88] Voor nadere eisen kan voor het Nederlandse recht worden aangesloten bij Landelijk Register van Gerechtelijke Deskundigen (LRGD).

Ten derde is er in de literatuur aandacht voor de kloof tussen de rechter en de expert of deskundige. De afgelopen jaren is er steeds meer aandacht voor forensisch onderzoek en de wijze waarop daarover wordt gerapporteerd. Rechters en experts of deskundigen volgen steeds meer opleidingen in het domein van de ander. Toch blijkt uit onderzoek dat de verschillen tussen wat de een zegt en de ander bedoelt nog niet te zijn opgelost.

Het vierde aandachtspunt komt voort uit het derde en ziet op de wijze waarop de expert of deskundige verslag doet van zijn bevindingen. In een goed onderzoeksverslag geeft de onderzoeker of deskundige niet alleen een verantwoord verslag van het verricht onderzoek maar houdt hij waar mogelijk ook rekening met zijn lezers. Dat betekent dat hij bepaalde bekende psychologische valkuilen zal moeten vermijden en zo ondubbelzinnig mogelijk zijn conclusies moet formuleren. Hij zal met andere woorden een weg moeten vinden tussen enerzijds een leesbaar en anderzijds een deskundig verantwoord onderzoeksverslag.

Met behulp van de hiervoor genoemde criteria kan de rechter een redelijke inschatting maken van de waarde van een door de rechthebbende opgestelde rapportage. Naarmate meer vragen positief worden beantwoord neemt de bewijswaarde toe.

Duidelijk is dat er voldoende redenen bestaan om de waarde van het door de rechthebbende ingebrachte rapport kritisch te benaderen en bij eerste zaken een deskundige te benoemen. De voorgaande vragen bieden hiervoor een raamwerk. Met een dergelijk verslag kan en zal de rechter rekening houden bij de waardering van stelplicht, bewijslast en uiteindelijk het watermerk als bewijsmiddel zelf.[89]

6.3 Waarderen van watermerken als bewijsmiddel

In de voorgaande paragraaf is gewezen op de lessen die geleerd kunnen worden uit de inzet van forensisch bewijs en verslagen van experts over dat bewijs. In deze paragraaf staan de elementen centraal waar ten aanzien van de watermerktechniek aandacht aan zou moeten worden besteed om aan de rapportage enige bewijskracht toe te kennen.

Om inzicht te krijgen in de betrouwbaarheid van de techniek is er in de literatuur gezocht naar vragen die gesteld zijn ten aanzien van de betrouwbaarheid van watermerktechnieken.

[88] Zie verder hoofdstuk 4.
[89] Zie ook De Hek 2013, p. 110 ten aanzien van de betekenis van accountantsrapporten in de civiele procedure.

Daarnaast zijn er verschillende gesprekken gevoerd met deskundigen.[90] De literatuur biedt echter geen volledig beeld van de bestaande watermerksystemen of -technieken. Een belangrijke reden daarvoor is dat van commerciële systemen niet altijd bekend is hoe deze functioneren. Er is echter weinig reden om aan te nemen dat de commerciële watermerksystemen niet op de eerder in hoofdstuk 4 gepresenteerde principes gebaseerd zijn en dat de vragen die in de literatuur worden gesteld wezenlijk verschillen met de vragen die ten aanzien van commerciële watermerksystemen gesteld kunnen worden. Aangenomen mag dan ook worden dat ook voor deze systemen de onderliggende principes en vragen hetzelfde zijn.

De huidige literatuur bestaat enerzijds uit beschrijvingen van nieuwe systemen en anderzijds uit specifieke technieken die aandacht hebben voor de basisvragen in het licht van nieuwe ontwikkelingen.[91] De literatuur geeft derhalve inzicht in de relevante vragen die moeten worden gesteld om te kunnen vaststellen of er in een voorliggend geval sprake is van een betrouwbaar watermerk. Doel van dit overzicht is niet het geven van een uitgebreide beschrijving van de laatste stand van watermerktechnieken maar om te komen tot een beeld van de relevante vragen in dit wetenschapsgebied. De expert of door de rechter benoemde deskundige dient er dan vooral toe om het watermerk te beoordelen naar de laatste stand van de wetenschap.

Uitgangspunt bij de waardering van watermerken vormt het wetenschappelijk uitgangspunt dat watermerken betrouwbaar zijn zolang men zich aan de basisprincipes houdt en de gebruikte techniek in de literatuur of wedstrijden niet is gekraakt (falsificatie).[92] Dit sluit in zoverre aan bij het beoordelen van bewijs in het recht dat zowel in het civiel als strafrecht ook als uitgangspunt geldt dat zolang forensisch bewijs naar de maatstaven van de betreffende wetenschap en praktijk plaatsvindt en er in beginsel geen reden is om aan te nemen dat het bewijs onbetrouwbaar is.[93]

Om uiteindelijk tot de conclusie te kunnen komen dat het watermerk als bewijsmiddel kan worden ingezet moet het een betrouwbaar bewijsmiddel blijken. Daarbij spelen in beginsel twee aspecten een belangrijke rol. Ten eerste moeten de gegevens die in het watermerk worden gestopt juist zijn. Ten tweede moet het watermerk als techniek betrouwbaar zijn. Dat wil zeggen dat dezelfde gegevens die in het watermerk zijn gestopt er ook weer uit te halen zijn. Het eerste deel is hiervoor (par. 6.2.1) besproken en ziet mede op de wijze waarop het gehele proces van verkrijging van gegevens tot analyseren en interpreteren is vormgegeven. Het deel waarin alleen de betrouwbaarheid van de techniek centraal staat en over welke

[90] P. Schelkens, A. Dooms, D. Bardyn (VUB, iMinds), R.L. Lagendijk (TU Delft) en W. Bus (Civolution).
[91] Hierbij moet gedacht worden aan vragen over robuustheid, zichtbaarheid, verweer tegen aanvallen, het gebruik van algoritmen, etc.
[92] De basisprincipes duiden op het feit dat de techniek juist moeten worden ingezet. Vanzelfsprekend werkt de techniek niet als men zich niet aan deze principes houdt. Een watermerktechniek is bijvoorbeeld weinig effectief wanneer zowel de techniek als de sleutel en het algoritme bekend zijn bij het publiek.
[93] Zie ook de (civiele) bewijswaarderingsmaatstaf van De Bock in par. 4.2.3.2.

onderwerpen tenminste gegevens zouden moeten worden opgenomen in de rapportage is in deze paragraaf nader onderzocht. Daartoe wordt aandacht besteed aan het valideren van watermerkensystemen en -technieken (par. 6.3.1) en aandacht gevraagd voor de meest aannemelijke technische verweren (par. 6.3.2).

6.3.1 Valideren van het gehele proces

Op grond van de literatuur zijn een aantal onderwerpen onderscheiden die van belang zijn voor het gebruik van watermerktechnieken en daarmee voor betrouwbare resultaten. In de rapportage zal om die reden aandacht moeten zijn voor deze onderwerpen. Centraal staat hier de gebruikte watermerktechniek.

Wijze waarop het hele systeem is ingericht

Het verslag zal vanwege de grote variëteit die in de praktijk mogelijk is een korte beschrijving moeten geven van het gehele proces. Dat wil zeggen vanaf het moment dat de gedaagde of verdachte zijn gegevens ter beschikking stelt tot het resultaat dat de gevonden code leidt tot de persoonsgegevens van de gedaagde of verdachte. Hij zal dan ook uitspraken moeten doen ten aanzien van zijn authenticatie- en verificatieproces.[94] In hoofdstuk twee is al eerder geconcludeerd dat het risico dat een watermerk de verkeerde uitkomst geeft in beginsel voort komt uit fouten die zijn gemaakt tijdens de authenticatieprocedure (bijv. door fouten in de administratie) of door een verkeerde toepassing van de techniek van watermerken. Hij zal daarbij vooral aandacht moeten hebben voor de wijze waarop het authenticatieproces in de praktijk werkt, technisch is ingericht en welke maatregelen zijn genomen om te voorkomen dat de (persoons)gegevens onjuist in het watermerk worden opgenomen. Er zal met andere woorden duidelijk moeten worden waarom de authenticatieprocedure en de gebruikte watermerksystemen betrouwbaar zijn en tot een betrouwbaar eindresultaat hebben geleid.[95] Hij zal daarbij ook rekenschap moeten geven van de meest aannemelijk aanvallen op het systeem en de kans dat die hebben plaatsgevonden. De rechthebbende zal er tot slot bij het maken van zijn verslag ook rekening mee moeten houden dat de gegevens waarnaar hij verwijst ook beschikbaar moeten zijn, zodat contra-expertise mogelijk is.

Valideren van de gebruikte techniek en processen

De rechthebbende zal moeten aangeven waarom de gebruikte technieken en processen voldoende betrouwbaar moeten worden geacht, bijvoorbeeld door middel van certificaten, testrapporten of verklaringen van deskundigen (par. 6.2.1). Het gaat hierbij zowel om het rechtvaardigen van keuzes die hij heeft gemaakt als om de technische en organisatorische

[94] Zie par. 2.2.5.
[95] In de praktijk kan dat op verschillende manieren. Zo is het mogelijk om een audit te laten uitvoeren in het kader van Identity and Access Management (IAM). Zie ook par. 6.2.1.

maatregelen die hij heeft getroffen om tot een betrouwbaar resultaat te komen. Hiermee wordt tevens inzicht gegeven in de kans op fouten in het onderzoeksproces.

Keuze voor een bepaald watermerk

Ten aanzien van de gehanteerde watermerkentechiek zal de rechthebbende in het licht van het doel, de schaal en het object (audio, video, afbeeldingen[96]) duidelijk moeten maken waarom hij juist voor deze watermerktechniek heeft gekozen.[97] Het gebruik van bijvoorbeeld een heel eenvoudige techniek als de "Least significant bit modification" is niet geschikt voor het beveiligen van waardevolle content omdat de techniek niet robuust genoeg is. De verantwoording moet duidelijk maken welke watermerktechniek (algoritme en sleutels) is gebruikt en hoe de gemaakte afwegingen zich verhouden tot het gekozen doel en het te gebruiken gastobject.[98] In de praktijk spelen naast de technische aspecten ook de kosten een belangrijke rol en zal de waarde van het object worden afgezet tegen de inspanningen. De verschillende keuzes die hij heeft moeten maken zal hij moeten verantwoorden. In de regel kan hij in het verslag volstaan met een korte verwijzing, wanneer hij verder beschikt over meer uitgebreide verslagen.

Nadat hij zijn keuze voor een bepaalde techniek heeft toegelicht zal er aandacht moeten zijn voor de vraag op welke wijze het watermerk is aangebracht, gedetecteerd en geanalyseerd. Een belangrijke vraag daarbij zal zijn of de gebruikte sleutels en algoritmen betrouwbaar zijn. Deze vraag kan vanuit de techniek beantwoord worden door te verwijzen naar literatuur of naar andere situaties waaruit kan worden opgemaakt dat deze zaken betrouwbaar zijn, zoals testrapporten.[99]

Het gaat er vooral om dat de gebruikte technieken en handelingen in de rapportage verantwoord worden. Risico’s, zoals Craver, Yeo & Yeung benoemen, dat het twijfels kan oproepen wanneer een watermerk eerst niet wordt gevonden, maar na het klaarmaken voor detectie wel wordt gevonden moeten hiermee worden voorkomen.[100] In de rapportage zal dan moeten worden uitgelegd dat het watermerksysteem bij het detecteren van het watermerk in staat moet zijn om aanpassingen, zoals rotatie, cropping, schalen, en gefuseerde content te

[96] Bij nieuwe bestandsformaten is het de vraag of de gebruikte watermerktechniek daarvoor geschikt is. In het algemeen werkt een watermerk voor beelden voor ieder formaat (jpeg, png, etc), omdat er altijd eerst wordt teruggegaan naar de RAW voorstelling. Voor nieuwe contenttypen, zoals 3D en holografie is het nog niet duidelijk hoe het watermerken plaats moet vinden.
[97] Zie par. 2.2.4.
[98] In de literatuur worden een aantal algemene eigenschappen van watermerken onderscheiden die onderling van invloed op elkaar kunnen zijn, zoals zichtbaarheid (perceptualtransparancy), opslagcapaciteit (payload), robuustheid (robustness), beveiliging (security) en de detectiemogelijkheden (zie par. 2.4). De eerste twee eigenschappen (zichtbaarheid en opslagcapaciteit) zijn weliswaar van invloed op de kwaliteit van watermerken, maar hebben geen directe invloed op de betrouwbaarheid van watermerken als juridisch bewijsmiddel.
[99] Een aantal van deze technieken zijn openbaar en worden bediscussieerd in openbare, vaak academische, bijeenkomsten. Een aantal andere technieken blijven onbekend omdat de ondernemingen belang hebben bij de geheimhouding van het gehele systeem inclusief het algoritme en sleutel.
[100]Zieo.m. Craver, Yeo &Yeung 1998, p. 48.

herkennen.[101] Dat kan betekenen dat men een geschaalde afbeelding terug moet brengen naar de originele afmetingen of het algoritme moet wijzen op de plaats waar hij moet zoeken wanneer bijvoorbeeld meerdere afbeeldingen in een fotocollage zijn opgenomen.[102] Het kan dus voorkomen dat voor de detectie begint het verdachte bestand eerst klaar gemaakt moet worden om te kunnen worden gedetecteerd. Dit hoeft voor de betrouwbaarheid van het watermerk geen probleem op te leveren zolang deze handeling maar goed beschreven en verantwoord is.

De rapportage zal dan ook duidelijk moeten maken dat met de gebruikte algoritme en sleutels de gevonden informatie kan worden achterhaald. Dat betekent dat het algoritme en sleutels volgens de wetenschappelijke maatstaven voldoende betrouwbaar moeten zijn. Dat betekent dat een expert van de andere partij met het gebruik van hetzelfde algoritme en de sleutel dezelfde informatie moet kunnen verkrijgen als wordt gesteld door rechthebbende.[103] Ook in gevallen waarin, zoals met commerciële systemen, de algoritmen en sleutels bedrijfsgeheim zijn, kunnen in het bewijsrecht voldoende maatregelen worden getroffen om een deskundige zijn werk te laten doen zonder dat de bedrijfsgeheimen worden prijsgegeven aan derden.[104]

Craver, Yeo & Yeung wijzen erop dat vanuit een wetenschappelijk standpunt er meerdere interpretatiemogelijkheden zijn terwijl rechthebbenden en hun advocaten graag substantieel bewijs willen zien in de rechtbank. Zij zagen op dat moment (1998) weinig juridische garanties op een succesvolle interpretatie mede in het licht van de verschillende (onbetrouwbare) methoden die er waren. In hoeverre zij daar nu anders tegen aankijken is niet bekend. Duidelijk is wel dat de techniek verder ontwikkeld is, maar ook de rechtspraak, zowel in de Verenigide Staten als in Nederland en België, is, veel meer dan in 1998 het geval was, bekend geraakt met forensisch bewijs. Zowel met de mogelijkheden als de beperkingen daarvan. In zowel Nederland als België geldt dat het uiteindelijk aan de rechter is om, eventueel met de hulp van een deskundige te bepalen of de juiste interpretatiemethode gekozen is.

Tot slot moet in de rapportage duidelijk worden wat de meest aannemelijke aanvallen zijn op de gebruikte watermerken en of en zo ja welk effect dat heeft op betrouwbaarheid van het watermerk als bewijsmiddel in de zaak waarin de rapportage wordt ingebracht. Welke

[101] Bijvoorbeeld doordat iets of iemand het algoritme duidelijk maakt waar het moet zoeken.
[102] Het opsporen (detection) van watermerken achten Voyatzis & Pitas 1999 (p. 1999) het meest cruciale deel van watermerksystemen. Craver, Yeo & Yeung (1998, p. 48) constateren dat het niet kunnen detecteren van het watermerk vaker het resultaat is van een gebrek aan een geavanceerd algoritme dat niet in staat is een verstoord of afgebroken (degraded) watermerk te detecteren dan van de afwezigheid van het watermerk zelf. Ook bij de gekozen detectie geldt een bepaalde trade-off tussen een verhoogde detectiekans en een verhoogde kans op vals alarm (zie o.m. Craver, Yeo &Yeung 1998, p. 49; Macq, Dittman & Delp 2004).
[103] Of zoals De Bock het in haar civielrechtelijke bewijswaarderingsmaatstaf noemt: De deskundige moet uit het watermerk op basis van zijn deskundigheid redelijkerwijs kunnen afleiden dat het feit zich heeft voorgedaan, en daaruit niet even goed kunnen afleiden dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan, terwijl zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden ontbreekt.
[104] Zie o.m. De Groot 2008 (diss.), p. 60; De Groot & Elbers 2008.

aanvallen het meest aannemelijk zijn zal mede afhangen van de gebruikte techniek en de tijd waarin het watermerk wordt onderzocht. In het verslag zal duidelijk moeten worden dat de watermerken voldoende weerstand konden bieden aan aanvallen die bij het aanbrengen het meest aannemelijk waren. Daarnaast zal het verslag melding moeten maken van de periode na het inbrengen tot aan het moment dat het betreffende watermerk is gedetecteerd. Het is immers ook mogelijk dat er bijvoorbeeld één jaar later aanvallen denkbaar zijn die bij het aanbrengen nog niet bekend waren en de betrouwbaarheid van de gebruikte watermerktechniek aantasten. Bijvoorbeeld omdat de publicatie over een bepaalde aanval pas is gepubliceerd na het aanbrengen van het watermerk. Het is aan de expert en eventueel de deskundige om te bepalen hoe waarschijnlijk het is dat een bepaalde aanval ook daadwerkelijk effect heeft gehad.

De rechthebbende zal extra aandacht moeten hebben voor aannemelijke verweren die mogelijk zijn voor het specifieke systeem dat hij heeft gekozen. Dit laat niet alleen zien dat het verslag grondig is geweest en hij kennis heeft van de zwakheden van zijn watermerksystemen, maar hiermee voorkomt hij ook dat het eenvoudig wordt om het verslag te bekritiseren.[105]

6.3.2 Aandacht voor aannemelijke verweren ten aanzien van de techniek

In hoofdstuk 4 is er reeds op gewezen dat de gedaagde drie typen aannemelijke verweren kan voeren.[106] Ten eerste het type verweer dat de gedaagde kan voeren zijn verweren ten aanzien van het gestelde feit. Bij dit type verweer betwist de gedaagde niet dat het bestand aan hem toebehoort, maar richt hij zich op alternatieve verklaringen die het gestelde feit verklaren. Ten tweede verweren die zich richten op de (juridische) toelaatbaarheid van watermerken als juridisch bewijsmiddel.[107] Ten derde verweren die zich richten op de betrouwbaarheid van het watermerk als bewijsmiddel. Bij deze verweren staat de vraag centraal onder welke omstandigheden watermerken de verkeerde uitkomst kunnen geven. De meeste aannemelijke verweren ten aanzien van de betrouwbaarheid van watermerken zijn verweren die zich richten op fouten in het authenticatieproces (verkeerde naam), fouten bij het inzetten van de techniek van watermerken waardoor er sprake kan zijn van een fout-positief, en het verweer dat iemand anders het bestand met ‘zijn’ traitor tracingscode en zonder zijn medeweten heeft verspreid (vals watermerk).

In deze paragraaf zal nader worden ingegaan op de meer technische verweren die de gedaagde kan voeren ten aanzien van de inzet van de techniek van watermerken.[108] Het komt dan anders

[105] Algemeen wordt ook in andere forensische disciplines aangenomen dat absoluut bewijs niet bestaat. Zie ook Broeders in een interview http://www.kennislink.nl/publicaties/absoluut-bewijs-is-altijd-verdacht.
[106] Zie in hoofdstuk 4 voornamelijk de paragraaf 4.2.2.
[107] Zie hoofdstuk 5.
[108] Hiermee wordt tevens duidelijk welke verweren het meest aannemelijk zijn. Dit is ook van belang voor de aan de deskundige te stellen vragen, waarmee de rechter een hogere graad van zekerheid kan verkrijgen ten aanzien van de vraag of het watermerk als bewijsmiddel betrouwbaar is of juist niet. Er is gekozen om geen model op te nemen van te stellen vragen anders dan in de vorm van de hier vermelde verweren, omdat een model

gezegd aan de op de vraag wanneer en onder welke omstandigheden watermerken de verkeerde uitkomst kunnen geven.

Behoudens algemene verweren ten aanzien van de gehanteerde methodiek, modellen en algoritmen zijn er drie verweren die extra de aandacht verdienen. Ten eerste kunnen er fouten zijn gemaakt in de administratie en meer in het bijzonder bij de authenticatie. Ten tweede het verweer dat het 'iemand anders' was en ten derde het verweer dat er sprake is van een fout-positief melding. Omdat het aannemelijke verweren betreft moet de rechthebbende daar naar mijn mening reeds op anticiperen in zijn verslag door aan deze onderdelen aandacht te besteden. Dat kan door ze expliciet te benoemen, maar ook door hier aandacht voor te hebben in de verantwoording van andere onderdelen van het proces.

Fouten bij de authenticatie

Het meest aannemelijke verweer ten aanzien van de authenticatie is gelegen in mogelijke fouten in de administratie van de gegevens. Argumenten voor deze stelling zouden moeten komen uit het verslag waarin de rechthebbende het watermerk als verslag presenteert. De gedaagde zal duidelijk moeten maken waar de fout zit en zijn verweer nader moeten motiveren. Tegen de achtergrond dat de rechthebbende niet graag toegang zal verlenen tot zijn gehele administratie en procedure is het denkbaar dat partijen uiteindelijk aan de rechter vragen een onafhankelijke deskundige te benoemen die onderzoek doet naar de fouten die de gedaagde gemotiveerd heeft gesteld.[109] In de praktijk is de kans groot dat het gehele proces van authenticatie tot uitgifte van de gewatermerkte content volledig geautomatiseerd is. De mate waarin de rechthebbende in zijn verslag de procedure en verschillende onderdelen daarvan heeft verantwoord zal van belang zijn bij het bepalen van de vraag hoe groot de kans is dat er fouten zijn gemaakt. Vanwege het belang van een dergelijke procedure voor de effectiviteit van het watermerk mag worden aangenomen dat de rechthebbende zijn procedure heeft laten testen op eventuele fouten. Het gebrek aan dergelijke testen is een indicatie voor gedaagde om hier gemotiveerd verweer tegen te voeren.

Het verslag zal tevens duidelijk moeten maken in welke mate het mogelijk is dat een rechthebbende zelf de verkeerde gegevens in het watermerk heeft kunnen plaatsen. Deze kans zal voor een belangrijk deel afhangen van de wijze waarop de administratie en het watermerken daarvan is ingericht.

In het verslag zal apart aandacht moeten zijn voor de mogelijkheid dat de administratie is gehackt waardoor er verkeerde gegevens vanuit de administratie als boodschap in het watermerk zijn opgenomen. De rechthebbende zal in zijn verslag aannemelijk moeten maken welke maatregelen hij heeft getroffen om te voorkomen dat onbevoegden toegang krijgen tot

van vragen te veel samen zou hangen met de gebruikte techniek en gemaakte keuzes ten aanzien van de techniek (par. 6.3.1) waardoor het model weinig handzaam meer zou zijn.

[109] Zie naar Nederlands civiel recht ook par. 4.2.1.1 (art. 843a Rv).

zijn systemen. In hoeverre die beschrijving voldoende is zal tijdens de zitting moeten blijken en afhangen van de stellingen die de gedaagde inneemt. Hoewel de stelling dat systemen gehackt zijn in theorie mogelijk is lijkt erop voorhand weinig reden om aan te nemen dat de administratie is gehackt.[110] Al zal het in de praktijk ook lastig zijn om aan te tonen dat de administratie wel gehackt is.

Vanzelfsprekend kunnen er ook fouten zijn ten aanzien van de authenticatie van de licentienemer maar dat is in een procedure minder waarschijnlijk. Dat is gelegen in het gebruik van het watermerk als bewijsmiddel. Voordat de rechthebbende de keuze maakt om het watermerk als juridisch bewijsmiddel in te brengen zal hij zich ervan vergewissen dat de naam die in het watermerk staat hem aannemelijk voorkomt.[111]

'Iemand anders'

Een van de meest aannemelijke technische verweren is het verweer dat iemand anders het bestand met 'zijn' traitor tracingscode en zonder zijn medeweten heeft verspreid. In hoofdstuk vier is reeds geconcludeerd dat de gedaagde of verdachte dit verweer tenminste aannemelijk zal moet maken om de rechter van zijn onschuld te overtuigen. De gedaagde of verdachte kan voor dit scenario verwijzen naar een onbekende derde of naar de rechthebbende die als enige de beschikking kan hebben over 'zijn' traitor tracingscode. Dat een derde het bestand met 'zijn' traitor tracingscode heeft verspreid is in theorie mogelijk, bijvoorbeeld doordat bij een zogenaamde 'collussion attack', waarbij meerdere aanvallers bestanden met elkaar vergelijken om de code zodanig te wijzigen dat hij niet naar hen leidt. Omdat het hier een aannemelijk verweer betreft zal de rechthebbende in zijn verslag moeten aangeven hoe groot hij die kans acht bij door hem ingezette watermerken.[112] In de regel zal die kans klein zijn vanwege de voortdurende aandacht hiervoor in de literatuur die ertoe bijdraagt dat technieken steeds beter worden en dergelijke kansen steeds kleiner worden. Wanneer de gedaagde op grond van het verslag bijzondere omstandigheden aanvoert ter zitting dan is het vervolgens aan de rechthebbende om daar op te reageren.

Ook voor het tweede scenario, waarin de rechthebbende frauduleus is, is aandacht in de literatuur.[113] Om dit verweer te kunnen pareren zal de rechthebbende vooraf maatregelen moeten hebben genomen en deze hebben beschreven in zijn verslag. Ten eerste zijn er technische maatregelen denkbaar in de vorm van een protocol.[114] Deze oplossingen kunnen er echter toe leiden dat het embedden langer duurt. In de praktijk wordt deze tijd begrensd door de tijd die consumenten bereid zijn te wachten op hun content. Hoe veel langer het

[110] De grote hack bij Sony uit 2014 laat zien dat het hacken van systemen van de entertainmentindustrie niet ondenkbaar is. Zie voor verweren ten aanzien van hacken, de paragraaf aannemelijke verweren in hoofdstuk 4. Zie in dit licht ook plicht die organisaties hebben inzake het melden van datalekken (Richtlijn 2009/136/EG).
[111] Bijvoorbeeld door de gegevens te vergelijken met andere gegevens, zoals de rekening waarvan betaald is. Watermerken die verwijzen naar fictieve namen zoals 'Pak me dan' of 'Donald Duck' worden eenvoudig niet als juridisch bewijsmiddel gebruikt.Zie ook par. 2.2.5.
[112] Zie ook het eerder genoemde element van het beschrijven van de meest aannemelijke aanvallen.
[113] Pfitzmann & Schunter 1996; Charpentier e.a. 2011.
[114] Zie Charpentier e.a. 2011. Dit is een vereenvoudigde weergave van een technisch complexe werkelijkheid.

embedden duurt zal afhangen van meerdere factoren (type, duur). Uiteindelijk zal de rechthebbende dit afzetten tegen de mogelijkheid dat hij zich voor een dergelijk verweer gesteld ziet. Ten tweede kan de rechthebbende er bij het inrichten van zijn systeem voor kiezen om een TTP te gebruiken die dan als enige beschikt over de code. Het verweer kan dan overigens nog steeds worden gevoerd. In die situatie zal de gedaagde of verdachte zich echter richten op de TTP als verspreider van het bestand. Het is dan aan de rechthebbende om duidelijk te maken waarom deze TTP betrouwbaar is. In de regel zal de rechter een TTP betrouwbaarder achten dan de rechthebbende zelf. Hiermee is vanzelfsprekend niet gezegd dat de rechthebbende niet betrouwbaar is. Het zal voor de gedaagde of verdachte, vanwege de belangen, echter eenvoudiger zijn twijfel te zaaien over de betrouwbaarheid van de rechthebbende dan over de betrouwbaarheid van de TTP.[115] Voor de boodschap van de gedaagde of verdachte maakt dat verder niet uit. Zijn boodschap blijft: 'ik was het niet'. Vooralsnog bestaan deze TTP's echter niet en is er ook geen aanwijzing dat deze erop korte termijn komen.

In hoeverre beide maatregelen voldoende zijn om de betrouwbaarheid van de resultaten van onderzoek op basis van het watermerk te waarborgen zal in de praktijk door een deskundige moeten worden beoordeeld. Het is aan de rechthebbende om zijn zienswijze over deze situatie alvast kenbaar te maken.

Fout-positief (fals-positive)

Een ander aannemelijk verweer ziet op de vraag of er sprake is van een zogenaamde fout-positief of false-positive. Het gaat dan om de situatie waarin de licentienemer ten onrechte als resultaat van het onderzoek naar voren is gekomen. Daarbij kunnen in beginsel twee situaties worden onderscheiden. De eerste situatie betreft de kans dat gegevens verkeerd zijn ingevoerd en in het watermerk zijn opgenomen.[116] De tweede situatie ziet op die gevallen waarin de detector ten onrechte aangeeft dat het object een watermerk bevat.[117] In hoofdstuk 2 is er al eerder op gewezen dat de rechthebbende aan de hand van verschillende parameters zelf bepaalt wat de kans is op een fout-positief resultaat.[118] Zo kan hij onder meer op basis van het aantal gebruikers zelf bepalen wat de kans is op een valse identificatie. In het verslag zal de expert moeten aangeven wat deze kans is en waarom deze in het voorliggende geval aanvaardbaar is.

Het is dan aan de wederpartij hiertegen verweer te voeren en/of aan een door de rechter benoemde deskundige om zich uit spreken over deze keuze en de mate waarin het resultaat

[115] Een TTP kan samenvattend helpen bewijs te leveren dat het bestand met watermerk naar gedaagde is gezonden, als verzendingsproces via TTP loopt of met kopie aan TTP. Een TTP kan echter geen bewijs leveren dat het bestand niet door derde op internet is gezet. Ten aanzien van het linken van de code is het de vraag hoe je iemand kan linken aan de code zonder het risico op belangenverstrengeling. Wie of wat garandeert de neutraliteit van de encodeur.
[116] Zie ook 2.2.5.
[117] Zie ook 2.4.1.
[118] Zie par. 2.4.1.

van die keuze van invloed is op de vraag hoe groot de kans is dat er sprake is van een false positive. Deze vraag is overigens niet specifiek voor watermerken, maar komt in meerdere forensische domeinen voor, zoals bij DNA-onderzoek.[119] Hoe groot de kans is op een false positive is in het algemeen niet te zeggen. Bij een fout-positief geeft de detector ten onrechte aan dat het object een watermerk bevat. Het aantal te verwachten fout positieven in een bepaald aantal runs van de detector wordt aangeduid met de term 'fals positive rate'.[120] Een dergelijke verwarring kan ontstaan doordat de detectiealgoritmen zelf ook werken op basis van kansberekening. Deze algoritme geven aan dat 'het is het meest waarschijnlijk dat onderstaande code in het werk zit'. Aan deze antwoorden worden door de onderzoekers grenzen gesteld, zodat het antwoord 'heel zeker' wordt. Aan de hand van verschillende parameters kan de rechthebbende tot een zekere hoogte zelf bepalen wat de kans is op een fout-positief resultaat. Zo kan hij onder meer op basis van het aantal gebruikers zelf bepalen wat de kans is op een valse identificatie. In de praktijk zal bepaald moeten worden welke kans op een fout-positief (tegen welke andere kosten) aanvaardbaar is en zal er uiteindelijk een keuze worden gemaakt. Deze keuze zal moeten worden verantwoord in de rapportage die de rechthebbende als bewijs aanvoert. Het staat de gedaagde dan vrij de door de rechthebbende genoemde kans gemotiveerd te betwisten.[121] Wanneer de rechter daarover vragen heeft kan hij daarvoor een deskundige aanstellen.[122]

Van alle bovenstaande verweren mag worden verwacht dat de rechthebbende hier aandacht aan besteedt in zijn verslag door duidelijk te maken waarom de kans klein moet worden geacht dat de eerder genoemde verweren een dusdanige invloed hebben op de resultaten dat deze onbetrouwbaar zouden zijn.[123] Een dergelijke verantwoording komt de waarheidsvinding ten goede alsmede het juridische proces van bewijsvoering omdat deze aannemelijke verweren dan reeds zijn besproken. In hoeverre de rechthebbende daar voldoende aandacht aan heeft besteed is dan aan de wederpartij en uiteindelijk de rechter.

6.4 Valkuilen bij het interpreteren van (betrouwbare) watermerken

De vraag of het watermerk een overtuigend bewijsmiddel kan zijn hangt niet alleen samen met de juridische vragen omtrent bewijs, maar voor een belangrijk deel ook met de overtuiging van de rechter.[124] Over de wijze waarop de rechter tot zijn beslissing komt is niet

[119] Zie voor DNA-onderzoek ook Meulenbroek 2003, p. 264.
[120] Miller, Cox & Bloom 1998, p. 75. Cox, e.a. 2007, p. 39.
[121] Zie voor de bewijsrisicoverdeling tussen partijen hoofdstuk 4 (par. 4.3.1, 4.4.1, etc).
[122] Zie voor het aanstellen van een deskundige door de rechter hoofdstuk 4 (par. 4.3.3.2, 4.4.3.2, etc)
[123] Ik spreek met opzet over een kans omdat er in dergelijke situaties weinig met zekerheid kan worden gezegd.
[124] Zie ook Hammerstein 2004 die als rechter schrijft: 'In de huidige praktijk berusten de beslissingen van rechters in hoge mate op een persoonlijke waardering die onder meer berust op hun ervaring en kennis van andere, soortgelijke gevallen. Deze afweging lijkt mij niet kwantificeerbaar, aangezien zij in hoge mate afhangt van intuïtie. Wigmore (1931, p. 3) maakte in zijn studie naar juridisch bewijs al onderscheid tussen de studie naar het bewijsrecht waar vragen rondom de toelaatbaarheid en wettelijke bewijskracht een rol spelen (law of evidence) en de studie naar het bewijs in het algemeen waarbij het proces van overtuiging door redeneren een rol speelt (rational process of proof) en zette in zijn werk de eerste stappen naar een 'science of judicial proof' voor rationele principes voor redeneren met bewijs onafhankelijk van de regels van het recht. Zie voor de scheiding

veel bekend. Juristen beschrijven de rechterlijke beslissing onder verwijzing naar Scholten veelal als een ongrijpbaar moment. De laatste jaren is vooral vanwege de gerechtelijke dwalingen in het strafrecht meer aandacht voor de wijze waarop rechters tot hun beslissing komen.[125] Deze dwalingen zijn in de literatuur veelal toegeschreven aan verschillende valkuilen waaraan mensen bloot staan bij het nemen van beslissingen.[126] Zij vormen niet alleen voor de waarheidsvinding een risico maar ook voor de rechthebbende die het watermerk wil inzetten als bewijs.[127] Hoewel de literatuur zich met name op het strafrecht richt, lijken rechterlijke dwalingen niet voorbehouden aan de strafrechter en mag worden aangenomen dat gelijke problemen en dwalingen zich ook in het civiel recht voordoen.[128] Vanwege de statistische wetmatigheden die gebruikt worden bij rapporten over watermerken richt de aandacht zich in deze paragraaf op de wijze waarop rechters tot hun beslissing komen (par. 6.4.1) en op valkuilen bij het gebruik van statistiek in rapportages (par. 6.4.2). Beide risico's moeten de rechter (en partijen) waakzaam maken bij het beoordelen van watermerken als bewijsmiddel.

In deze paragraaf wordt, bij gebrek aan onderzoek in Nederland, gebruik gemaakt van onderzoek dat is verricht in de Verenigde Staten. Hierbij moet worden opgemerkt dat niet altijd duidelijk is of de resultaten uit die onderzoeken ook gelding hebben voor de wijze waarop de Nederlandse of Belgische rechter tot een beslissing komt. Aangenomen wordt dat veel van de gesignaleerde valkuilen in beginsel een vrij universele werking hebben.[129]

tussen de rationele en juridische aspecten van bewijs de belangrijke rationalistische traditie uit de Anglo-Amerikaanse rechtsfilosofie Bex & Verheij 2010. In het Engels is er een mooi onderscheid tussen evidence en proof, waarbij het laatste het vaststaande feit vormt en het eerste die mogelijkheid biedt.

[125] Met de term rechterlijke dwaling wordt hier verwezen naar een verkeerde vaststelling van feiten en niet op rechtskwesties waartegen in beginsel wel cassatie open staat. Rechterlijke dwaling vormen met name in die zaken een probleem waarin een verkeerde vaststelling van feiten leidt tot een onjuiste uitspraak, dat wil zeggen dat de verdachte ten onrechte wordt veroordeeld (vals positief) of ten onrechte wordt vrijgesproken (vals negatief). Bekende voorbeelden van gerechtelijke dwalingen zijn de Puttense Moordzaak (Hof Leeuwarden 24 april 2002, ECLI:NL:GHLEE:2002:AE1877, NS 2002, 182), Schiedammer Parkmoord (Hof Amsterdam 4 mei 2006, ECLI:NL:GHAMS:2006:AW8270) en Lucia de B. (Hof Arnhem 14 april 2010, ECLI:NL:GHARN:2010:BM0876, NJ 2010, 363 m. nt. P.A.M. Mevis).

[126] Zie voor een overzicht van de literatuur over de discussie over de wijze waarop rechters tot hun oordeel komen en de juridische waarheidsvinding o.m. Rozemond 2010. Zie voor bewijswaardering en psychologische inzichten in het civiel recht Enneking, Giesen & Rijnhout 2013.

[127] In de praktijk zal de rechthebbende vooral geïnteresseerd zijn in een positieve uitkomst van het geschil. Of zoals een bekende advocatenanekdote luidt over een advocaat die zijn cliënt belt met de uitslag van een rechtszaak en zijn cliënt mededeelt: 'het recht heeft gezegevierd', waarop de cliënt antwoordt: 'stel onmiddellijk hoger beroep in'. Door de toenemende aandacht voor (rechts)psychologie komt er ook steeds meer kritiek. De kritiek richt zich voornamelijk op de constatering dat de hypothesetoetsting, inclusief de toetsing aan de alternatieve hypothese die de eerder genoemde psychologen voorstellen door hen zelf ook niet wordt gevolgd onder meer door bepaalde informatie uit de door hun besproken dossiers weg te laten. Zie o.m. Arlan 2011; Rozemond 2010. Daarnaast zouden de rechtspsychologen niet goed op de hoogte zijn van strafrechtelijke begrippen. Rozemond komt daarnaast tot de conclusie dat ook getrainde rechtspsychologen blijkbaar dezelfde vergissingen kunnen maken als zij de rechters verwijten.

[128] Asser (2012) wijst in het recente Asserdeel Bewijs in het kader van de betrouwbaarheid van bewijsmiddelen wel op hoe lastig het in dit licht is om feiten vast te stellen. (p. 275, 277, 279). Zie ook Giard 2011, Borgers & Van Boom 2005. In het civiele recht lijkt de wisselwerking tussen recht en psychologie veel meer op het terrein van de werking van het recht en procedural justice te liggen. Zie voor voorbeelden en literatuurverwijzingen over (civiel)recht en psychologie in Nederland, Giessen 2010 (WPNR); Van Boom, Giesen en Verheij 2013.

[129] De door mij geconsulteerde psychologen merken op dat vanzelfsprekend onderzoek onder Nederlandse dan wel Belgische rechters betrouwbaarder is en ook dan pas de vraag kan worden beantwoord of er daadwerkelijk sprake is van verschillen.

Rachlinski maakt door vergelijkbaar (deel)onderzoek in Nederland uit te voeren in ieder geval duidelijk dat er verschillen kunnen zijn.[130] Deze verschillen zouden volgens hem deels verklaard kunnen worden door het verschil in rechtssysteem. Zo werken Amerikaanse rechters binnen een systeem waar via hoor en wederhoor het geschil en de bewijzen aan partijen wordt overgelaten (adversarial system). Hierdoor hoeven zij zelden een keuze te maken welk bewijs zij volgen. Terwijl in Nederland de rechter meer zelf aan waarheidsvinding doet en gewend is keuzes te maken welk bewijs hij volgt. Door het jurysysteem wordt de waardering van bewijs in de Verenigde Staten niet altijd aan de rechter overgelaten.[131] Onderzoek naar jury's is in het kader van de wijze waarop mensen beslissen over juridisch bewijs ook aan beperkingen onderhevig omdat rechters op hun beurt jury's in civiele zaken instrueren om de zaak element bij element te beoordelen. In de praktijk beoordeelt men dat op basis van meer waarschijnlijk dan niet.[132] Minder duidelijk is of er ook andere verschillen zijn die van invloed zijn op resultaten wanneer het onderzoek bij Nederlandse rechters zou worden uitgevoerd. Onduidelijk is ook hoe verschillen doorwerken en op welke terreinen. De rechtelijke dwalingen in het strafrecht en de onderzoeken daarnaar maken aannemelijk dat een aantal valkuilen ook geldt voor Nederlandse rechters.[133] De mate waarin Nederlandse rechters vatbaar zijn voor bepaalde valkuilen is mede afhankelijk van hun rol in het rechtssysteem en om die reden moeten resultaten uit Amerikaans onderzoek met enige terughoudendheid worden benaderd. Over de vraag hoe rechters beslissen bestaat veel onderzoek maar even zoveel kritiek daarop.[134] Naast deze onderzoeken kan nog aansluiting worden gezocht bij individuele rechters die zich daarover in de literatuur uitlaten. Het probleem van individuele opvattingen van rechters blijft dat het de opvatting of zienswijze van een enkel individu betreft, terwijl onderzoek naar een groep rechters evenmin uitsluitsel geeft over individuele zaken. Ondanks de hier genoemde beperkingen bieden de verschillende Amerikaanse onderzoeken meer wetenschappelijke gefundeerde inzichten dan mogelijk zou zijn op basis van enkel de huidige (juridische) literatuur.

Een ander belangrijk voorbehoud ten aanzien van de hier gebruikte onderzoeken is dat, zoals eerder besproken, onderzoeken aan verschillende beperkingen onderhevig zijn.[135] De hier te bespreken valkuilen ten aanzien van forensisch onderzoek en het gebruik van getallen zijn gebaseerd op resultaten van wetenschappelijk onderzoek, maar daarmee is niet gezegd dat alle

[130]Zie Rachlinski (2012, p. 19) die in een onderzoek naar confirmatiebias stelt dat Nederlandse rechters veel beter scoren op kort gezegd het selecteren van relevant bewijs dan hun Amerikaanse collega's. Voor inhoudelijke kritiek zie o.m. Rassin 2012.

[131] Ook in België kent men in een jury-syteem. Daar wordt echter enkel nog bij zeer zware misdrijven gebruik van gemaakt.

[132] Van Stekelenburg 2009 (diss.), p. 12 onder verwijzing naar G.C. Lilly, Principles of Evidence, St. Paul: Thomson West 2006, p. 387; zie ook Clermont 2012.

[133] Van een rechtelijke dwaling is alleen sprake wanneer onterecht wordt veroordeeld. In het strafrecht geldt immers dat de rechter bij twijfel op grond van zijn overtuiging de verdachte vrijspreekt.

[134] Klijn 2010 geeft een mooi overzicht van de kritiek op de poging van Posner om inzicht te geven in 'How Judges Think'.

[135] Zie par. 1.3.1. Zie voor beperkingen ten aanzien van het gebruik van psychologisch onderzoek en bewijswaardering ook Enneking, Giesen & Rijnhout 2013, p. 1021.

rechters ook in deze valkuilen trappen. De beschrijving van de valkuilen moet worden begrepen in termen van risico's ten aanzien van het gebruik van watermerken.

Naast de bewijsrechtelijke beperkingen en psychologische valkuilen zijn er vanzelfsprekend ook andere praktische beperkingen waarmee de rechter wordt geconfronteerd wanneer hij tot een bewijsoordeel wil komen dat overeenkomt met de werkelijkheid, zoals capaciteitstekorten, wetenschappelijke onduidelijkheid ten aanzien van een onderwerp, elkaar tegensprekende deskundigen en het belang of de wens van de procesdeelnemers.

6.4.1 Het proces van juridisch beslissen over bewijs

Het proces van juridisch beslissen over bewijs moet uiteindelijk leiden tot een beslissing waarvan de rechter overtuigd is. Over de wijze waarop rechters tot hun beslissing en overtuiging komen wordt langzaam meer bekend.

Het algemene beeld van de rechterlijke oordeelsvorming laat zich vangen in het syllogisme waarin de rechter de in de wet gevonden toepasselijke rechtsregel (maior) toepast op de concrete feiten (minor) en dat daaruit het rechterlijk oordeel voortkomt (conclusio).[136] In de juridische literatuur wordt algemeen aangenomen dat dit beeld te eenvoudig is vanwege de suggestie dat de beslissing logisch-dwingend voortvloeit uit de feiten vaststelling en de toepassing van de juiste rechtsregel.[137] Scholten benadrukt dan ook dat de rechterlijke beslissing altijd berust op een ongrijpbaar moment, een sprong: 'In waarheid vinden wij ze door zoveel mogelijk gegevens samen te brengen en dan te beslissen. In de beslissing zit ten slotte altijd een sprong.'[138] Een tweede punt van kritiek op dit beeld van syllogisme is dat er altijd sprake is van een continu proces van beginnen, bijstellen, toespitsen, opnieuw bekijken en uiteindelijk de knoop doorhakken, zoals Vranken het proces van rechterlijke oordeelsvorming beschrijft.[139] Er vindt voortdurend een wisselwerking plaats tussen feiten en recht, omdat de feitenvaststelling alleen kan plaatsvinden vanuit een bepaalde context en vanuit een bepaalde rechtsregel.[140] Een derde punt van kritiek is dat al bij de start van de te vormen beslissing, de te nemen beslissing van belang is. 'Het resultaat van de oordeelsvorming moet immers een aanvaardbare beslissing zijn die past in het rechtssysteem en voldoet aan de eisen van rechtvaardigheid.'[141] Voor de vraag hoe rechters tot hun beslissing komen moeten wij uit de rechtswetenschappelijke literatuur stappen. In Nederland

[136] De Bock 2011, p. 5; Visser 2009, p. 2; Asser 2005, p. 192; Telders 1937, p. 103-112; 1947, p. 159-167.
[137] Zie o.m. Telders 1937, p. 165-167; Asser-Scholten 1974, p. 76, 129; Crombag, De Wijkerslooth en Cohen 1977, p. 19; De Bock 2011, p. 5; Visser 2011b, p. 321.
[138] Scholten 1974, p. 76.
[139] Vranken 1995, p. 73.
[140] Zie o.m. Scholten 1974, p. 120; De Bock p. 6.
[141] De Bock 2011, p. 6 of zoals De Groot (2008, p. 2) stelt: 'Een rechterlijke beslissing moet begrijpelijk zijn met het hoofd, invoelbaar met het hart, en uitvoerbaar met de benen.'

hebben de psychologen Crombag, Van Koppen & Wagenaar in 1993 in hun boek Dubieuze zaken aandacht gevraagd voor de psychologie van strafrechtelijk bewijs.[142]

Naar aanleiding van een aantal rechterlijke dwalingen, zoals de Puttense Moordzaak[143], Schiedammer Parkmoord[144] en Lucia de B[145] is de aandacht voor de wijze waarop rechters, maar ook het OM en de politie tot bepaalde beslissingen komen, toegenomen.[146]
De belangrijkste uitkomst is dat er te weinig aandacht is geweest voor een alternatieve hypothese in relatie tot het bewijs.[147] Of anders gezegd er is te weinig aandacht geweest voor een andere verklaring voor hetzelfde feitencomplex. Vanuit de psychologie is veel aandacht voor kort gezegd de valkuilen die mensen tegenkomen bij het nemen van beslissingen. In verschillende disciplines wordt aan modellen gewerkt om deze valkuilen te vermijden en ook aandacht te hebben voor alternatieve hypothesen.[148] Hoewel op het eerste gezicht dit vooral een kwestie lijkt van bewijswaardering is het onderwerp van belang voor watermerken. De psychologische processen zijn immers van invloed op de wijze waarop de rechter beslist over watermerken. Vanuit het perspectief van de rechthebbende als gebruiker van het watermerk kan het licht laten schijnen op de risico's die het watermerk als bewijsmiddel met zich meebrengt. Terwijl het vanuit het perspectief van de waarheidsvinding risico's oplevert ten aanzien van de juiste vaststelling.

---

[142] In de Verenigde Staten wordt al langer onderzoek gedaan naar de wijze waarop rechters tot beslissingen komen.
[143] Hof Leeuwarden 24 april 2002, ECLI:NL:GHLEE:2002:AE1877, NS 2002, 182 (Vrijspraak Puttense Moordzaak). Zie voor een chronologische volgorde en alle instanties het dossier op rechtspraak.nl.
[144] Hof Amsterdam 4 mei 2006, ECLI:NL:GHAMS:2006:AW8270 (Niet ontvankelijk OM: Schiedammer Parkmoord); HR 2 oktober 2007, ECLI:NL:HR:2007:BA5831, NJ 2007, 545 (Cassatie inzake motivering).
[145] Hof Arnhem 14 april 2010, ECLI:NL:GHARN:2010:BM0876, NJ 2010, 363 m.nt. P.A.M. Mevis (Vrijspraak Lucia de B.). Zie voor een chronologische volgorde en alle instanties het dossier op rechtspraak.nl.
[146] Zie o.m. Van den Emster en Verburg 2007 die vanuit de rechtbank en het hof verslag doen van een intern onderzoek. Dit heeft inmiddels bij het OM en de rechtelijke macht ook geleid tot meer opleidingen die hier specifiek aandacht voor vragen. Gross (1987, 1996) laat in de Verenigde Staten zien dat de kans groter is dat er in grote zaken rechterlijke dwalingen voorkomen dan in kleine zaken. Voor psychologische (en juridische) processen die daaraan ten grondslag liggen, zie o.m. Van Koppen, 2011. Zie ook Frielink 2011 (Strafblad 2011/2, jrg 9), die stelt dat de kwaliteitsslag die het OM in de opsporing en vervolging heeft gemaakt na de Schiedammer parkmoord om rechterlijke dwalingen tegen te gaan, ten koste is gegaan 'van de aandacht voor een veel grotere groep 'lichtere' zaken'.
[147] Zie voor de uitkomsten naar aanleiding van Schiedammer Parkmoord, het rapport Posthumus 2005.
[148] De drie hoofdbenaderingen zijn: het argumentatie (filosofie), narratief (psychologie) en het statische (wiskunde) perspectief. Bij een argumentatief perspectief ligt de nadruk op het construeren en evalueren van argumenten. Wigmore was de eerste die zijn charting method argumenten systematisch in schema's onderbracht om de verhoudingen te bepalen en hun waarde. De beweging na Wigmore is bekend als de New Evidence Scholars (Toulmin; Anderson, Schum en Twining). Bij een narratief perspectief ligt vooral op het construeren en vergelijken van verschillende verhalen of scenario's over de werkelijke toedracht. De losse feiten of gebeurtenissen leiden uiteindelijk tot een verhaal (Pennington en Hastie 1993). In Nederland hebben Crombag, Van Koppen en Wagenaar (1994) dit perspectief nader uitgewerkt in hun theorie over verhaal en verankering. Daarbij dient een goed verhaal niet alleen deze structuur te hebben maar ook verankerd zijn door algemene regels waardoor het verhaal aansluit bij onze kennis en verwachtingen over de wereld om ons heen. Een statistisch perspectief richt zich op het toekennen van een waarde aan bewijsmiddelen op basis van berekingen. Het idee achter de statistiek is dat een hypothese wordt geformuleerd ten aanzien van het feit en daarna de kans (likelyhood ratio) wordt berekend dat het feit zich heeft voorgedaan, bijvoorbeeld bij een DNA-match. Zie o.m. Bex & Verheij 2010, p. 967 en uitgebreid Bex in zijn dissertatie (2009); Van Koppen 2011, p. 35.

In de juridische literatuur wordt algemeen aangenomen dat de rechter naast het bewijsrecht en zijn motiveringsplicht bij zijn beslissingsproces gebruik maakt van zijn rechterlijke 'intuïtie' of 'Vorverständnis'.[149] Wat overtuigend is, is echter ook persoonsgebonden.[150] Experimenteel onderzoek onder Amerikaanse rechters over de verhouding tussen intuïtie en rationeel redeneren laat zien dat rechters net als iedereen voor het nemen van beslissingen gebruik maken van twee cognitieve systemen: intuïtie en rationeel redeneren.[151] Daarbij lijkt met name de intuïtie een sterk effect te hebben op het beslisproces. Guthrie e.a. wijzen er daarbij op dat de intuïtie prima kan werken in de ene zaak, maar in andere zaken kan leiden tot verkeerde en onrechtvaardige uitkomsten.[152] In de literatuur wordt het nagenoeg ondenkbaar geacht dat de rechter zijn intuïtie kan onderdrukken. Daarvoor wordt een aantal redenen gegeven: het intuïtieve systeem werkt vaak onbewust en snel, het is in staat redeneringen te sturen en mensen te overtuigen waardoor er niet direct een aanleiding wordt gezien om waakzaam te zijn. Mensen maken bij het nemen van complexe beslissingen graag gebruik maken van eenvoudige regels en mentale 'shortcuts'.[153] Ook wanneer de intuïtie mensen naar foute conclusies leidt zijn zij behoorlijk zeker van de juistheid ervan.[154] Rachlinski maakt duidelijk dat intuïtie ook nodig is voor het creëren van voldoende (zelf)vertrouwen om keuzes te maken en tot een beslissing te komen.[155] Ook in de juridische literatuur wordt, niet anders dan bij andere mensen, getwijfeld aan het vermogen van de rechter om kritisch en rationeel te zijn.[156]

Vanuit de psychologische literatuur wordt er vooral op gewezen dat het noodzakelijk is dat rechters zich bewust zijn van hun beslissingsstrategie en bijbehorende valkuilen.[157] Rachlinski pleit dan ook voor een combinatie van intuïtie en redeneren en verwijst daarbij naar ingenieurs en wiskundigen die volgens hem zich dit meer eigen hebben gemaakt dan juristen.[158] De valkuilen of nadelen van het intuïtieve denken komen naar voren in de

[149] Esser 1972, p. 43l; Scholten 1974, p. 132; Barendrecht 1992, p. 179; Visser 2009, p. 7; Cleiren 2010, p. 264. Academisch psychologen moeten daarentegen niets van 'intuïtie' (Grove e.a. 2000). Volgens Cleiren (2010, p. 262) geven Nederlandse strafrechters de notie van de rechterlijke overtuiging vorm in termen van intuïtie, fingerspitzengefühl, ervaring en praktische wijsheid. Zie ook Crombag, De Wijkerslooth en Cohen 1977 (p. 19) die tot de conclusie komen dat rechters 'niet volgens de regels van de 'akademischeMethodenlehre' van problemen naar oplossing redeneren, maar zich op grond van hun 'Vorverständnis' vrijwel onmiddellijk een beeld van de oplossing vormen, die zij pas daarna met juridische argumenten proberen te onderbouwen. Tversky & Kahneman 1974, p. 1124-1131. Rassin 2012, p. 11 merkt op dat deze termen voor menig wetenschapper al te abstract zijn en dat veel academisch psychologen niets moeten hebben van 'intuitie' vanwege het gebrek aan betrouwbaarheid daarvan.
[150] Rassin 2010, p. 208.
[151] Guhtrie, Rachlinski & Wistrich 2007; Kahneman 2011.
[152] Guthrie, Rachlinski & Wistrich 2001; Guthrie 2007, p. 141; Rachlinski 2012.
[153] Rachlinski 2012, p. 15-16; Kahneman 2011; Tversky & Kahneman 1974, p. 1124-1131
[154] Rachlinski 2012, p. 15-16; Rassin 2012, p. 12.
[155] Rachlinski 2012,p. 15-16. Hij verwijst naar een onderzoek van Damasio (1994) met mensen die een zwak ontwikkeld intuitief en affectief beoordelingssysteem hebben en weliswaar alle aspecten van de zaak kunnen benoemen maar niet tot een oordeel kunnen komen.
[156] Zie Aben 2010a, p. 85.
[157] Guhtrie, Rachlinski & Wistrich 2007; Kahneman 2011; zie vanuit de forensische literatuur ook Broeders 2010 A, p. 6.
[158] Rachlinski (2012, p. 19) verwijst tevens naar een onderzoek waaruit blijkt dat rechters dit niet doen. Hij gaat er in zijn test vanuit dat als rechters dit beter doen zij de test beter zouden moeten maken dan MIT-studenten die

gevoeligheid voor, verankering, framing en de moeite die mensen hebben met statistische wetmatigheden.[159] Met name de wijze waarop rechters omgaan met getallen en statistische wetmatigheden is van belang voor de waardering van watermerken en de mate waarin de rechter overtuigd raakt van het bewijs dat een watermerk kan bieden. Voor watermerken moet daarbij vooral worden gedacht aan de inhoud van een rapportage en de wijze waarop een expert zijn verslag doet.

6.4.2 De invloed van getallen

Verschillende onderzoeken laten drie wijzen zien waarop de beslissing van rechter beïnvloed kan worden door het gebruik van getallen.

Ten eerste kunnen numerieke referentiepunten als ankers dienen (verankering).[160] Ook in die gevallen waarin het gebruik arbitrair, irrelevant of zelfs absurd is.[161] Zo werd in een Duits onderzoek aan rechters gevraagd om bij de veroordeling van een verdachte eerst twee dobbelstenen te gooien en dit getal in te vullen als hoogte van de eis van de Officier van Justitie waarna zij later mochten beslissen over de hoogte van de straf. De rechters die hoge ogen gooiden deelden vervolgens hogere straffen uit dan rechters die lagere ogen gooiden.[162] Ook was een groep Canadese rechters bereid een hogere schadevergoeding toe te kennen na het zien van een verklaring waarin iemand $415.300 'compensatory damage' had gekregen dan in het geval waarin er slechts sprake was van compensatory damage zonder een bedrag daarbij.[163]

Ten tweede kunnen bij de presentatie gebruikte percentages van invloed zijn op de wijze waarop de rechter tot zijn beslissing komt (framing). In een experiment werd rechters op een bijeenkomst gevraagd bij welke kans op geweld zij opsluiting gerechtvaardigd achten.[164] Een groep kreeg de vraag in procenten (1%, 8%, 26%, 56% en 75%) en een andere groep kreeg dezelfde vraag gesteld in getallen van honderd (1 op 100, 8 op 100, etc,). Deze eerste groep legde de drempel gemiddeld bij 26% en de andere groep bij 8 op 100 (12,5 %). Voor deze laatste groep werd hiermee direct duidelijk om hoeveel mensen het gaat, terwijl die intuïtieve aandacht er niet lijkt te zijn bij de groep die percentages kreeg. Rassin geeft een ander voorbeeld, namelijk dat mensen een loterij aantrekkelijker vinden om mee te doen wanneer er

hij ziet als een groep die dit enigszins beheerst. Opvallend is overigens dat de 'Dutch Trial Judges' eindigen na de MIT-studenten en het beter doen dan hun Canadese en Amerikaanse collega's. 'On the whole, most groups of trial judges respond similarly to well-educated undergraduates at elite universities.'

[159] Zie o.m. Rassin, p. 11-12. Verankering ziet op het nemen van beslissingen waarbij mensen onbewust beïnvloed worden door informatie die in werkelijkheid irrelevant is. Framing verwijst kort gezegd naar de mate waarin mensen gevoelig zijn voor de wijze waarop iets gepresenteerd wordt. Zie o.m. Rachlinski 2012, p. 21 en de daar aangehaalde voorbeelden en literatuur.

[160] Zie o.m. Enneking, Giesen & Rijnhout 2013; Rachlinski 2012, p. 24 en de daar aangehaalde voorbeelden.

[161] Rachlinksi 2012, p. 27.

[162] Englich 2006, p. 194.

[163] Guthrie, Rachlinski & Wistrich 2009, p. 1477-1530.

[164] Monahan & Silver 2003

een winkans is van 30% dan aan een variant waarbij er 70% kans is dat men niets wint. In werkelijkheid is de winkans natuurlijk even groot.[165]

Ten derde wordt er gewezen op valkuilen ten aanzien van statische wetmatigheden. Zo blijkt dat sommige mensen de kans om blind een rode knikker uit een zak te trekken groter schatten bij een zak met 10 rode en 90 blauwe knikkers dan bij een zak met 1 rode en 9 blauwe.[166] Dit is bij rechters niet anders. Dat probleem kan zich voordoen bij het interpreteren van rapportages rondom het watermerk, zoals deze zich nu voordoen rondom DNA-profielen. Rassin wijst erop ‘‘hoe moeilijk het is om het verschil te onderkennen tussen de conclusie dat ‘de kans om dit DNA-profiel te vinden, aannemend dat de verdachte de dader is, duizend keer zo groot is als de kans om het niet te vinden’ en die dat ‘de kans dat de verdachte inderdaad de dader is duizend keer zo groot is als dat hij dat niet is’.’[167] Ook in de forensische literatuur wordt vaak gewezen op een aantal valkuilen die bekend is bij het interpreteren van lage matchkansen uit DNA-onderzoek.[168]Sjerps en Kloosterman noemen de ‘prosecutor’s fallacy’ en de ‘defence (attorney’s) fallacy’ als bekendste en gevaarlijkste.[169] In beide gevallen gaat het om een denkfout die ervoor zorgt dat de stelling sterker naar voren komt dan hij in werkelijkheid is.[170] Taverne e.a. merken op dat het op dit moment niet bekend in hoeveel zaken het maken van de ‘prosecutor’s fallacy’ tot daadwerkelijke onjuiste beslissingen heeft geleid. Zij sluiten niet uit dat deze denkfout tot op zekere hoogte een academisch probleem betreft.[171]

De ‘prosecutor’s fallacy’ dankt zijn naam aan het voorbeeld van een openbaar aanklager. Hij was van mening dat als een verdachte met de dader overeenkomt op een bepaald kenmerk, bijvoorbeeld het type bloed, dat een relatieve frequentie heeft van 10% in de bevolkingsgroep waaruit de dader verondersteld wordt afkomstig te zijn, de kans dat deze verdacht de dader is dan (100%-10%) 90% bedraagt.[172] De aanklager komt terecht tot de conclusie dat er een kans

[165] Rassin 2012, p. 14.
[166] Rassin 2012, p. 15; Rachlinski 2012, p. 24. Ook het gebrek aan rekenkundig vermogen kan van invloed zijn op de bewijswaarde die de rechter aan een bewijsmiddel toekent. Zie bijvoorbeeld de annotatie van Spoor onder hof ’s-Hertogenbosch 8 juni 2004, ECLI:NL:GHSHE:2004:AP2368 , AMI 2004/14 (Lancôme / Kecofa) onder 5, waarin hij aangeeft dat een in het overlegde rapport gemaakte vergelijking met wat schoolrekenen al aan had kunnen tonen dat het zodanige nonsens was hij ieder vertrouwen in de rest van het rapport voorgoed teniet had kunnen, en wat hem betreft ook had horen te doen.
[167] Rassin 2012, p. 12. De eerste regel geeft de kans aan dat het DNA-profiel dat van de dader is 1000x groter is, aangenomen dat hij de dader is. De tweede kans geeft de kans aan dat de dader het heeft gedaan ten opzichte van de kans dat hij het niet heeft gedaan. Bij het eerst genoemde geval zullen veel mensen het tweede geval voor ogen hebben.
[168] Zie o.m. Broeder 2003, p, 249, Sjerps & Kloosterman 2005, p. 320; Sjerps 2008, p. 484.
[169] De prosecutor’s fallacy is in de literatuur ook bekendals ‘fallacy of the transposed conditional’. Zie verder Thompson & Schuman 1987; Broeders 2003 (diss.) p. 249; Sjerps & Kloosterman 2005, p. 320; Sjerps 2008, p. 484. Broeders 2003 (diss.), p. 255 geeft enkele voorbeelden in de Nederlandse rechtspraak en geeft aan dat onbekend is hoe vaak de rechter zich in Nederland schuldig maakt aan deze fallacy. Onderzoek waaruit thans een andere conclusie kan worden getrokken is mij niet bekend.
[170] Zie voor rechters die in Nederland dezelfde fout maken, o.m. Hof Amsterdam 26 april 2001, ECLI:NL:GHAMS:2001:AD4264, NJ 2001, 399; HR 10 december 2002, ECLI:NL:HR:2002:AE6863. Zie voor meer voorbeelden naar Amerikaans recht, Broeders 2003, p. 252 en de daar aangehaalde voorbeelden.
[171] Taverne e.a. 2013, p. 42.
[172] Thompson & Schumann 1987; Het voorbeeld en de beschrijving is ontleend aan Broeders 2003, p. 249;

van 10% is op een overeenkomst als de verdachte onschuldig is. De daarop volgende conclusie dat dan de kans dat de verdachte schuldig is 90% bedraagt, kan echter niet worden getrokken. Deze laatste conclusie zou immers alleen geldig zijn als er 10% kans is dat de verdachte onschuldig is. Broeders wijst erop dat het hier niet gaat over de kans op schuld maar over de kans op een overeenkomst op basis van het bloedtype.[173] De aanklager redeneert alsof de kans op onschuld bekend is (gegeven een bepaald bloedtype) in plaats van de kans op een overeenkomst (gegeven de onschuld). De aanklager keert dus de kans dat er een overeenkomst is als de verdachte onschuldig is om in de kans dat de verdachte (on)schuldig is als zijn bloed overeenkomt.[174] Een ander veelgebruikt voorbeeld is dat als het regent straten nat worden dit nog niet betekent dat als straten nat zijn het geregend heeft. De oorzaak daarvan kan ook gelegen zijn in andere oorzaken zoals kinderen die met water hebben gespeeld. Dat het in de praktijk lastig blijkt laten ook Taverne e.a. (2013) zien.[175] In hun onderzoek naar DNA-rapporten blijkt dat ook na jaren DNA-onderzoek, nog driekwart van de respondenten de 'prosecutor's fallacy' heeft gemaakt. Ook nu nog laten zij zien moeite te hebben om de conclusies van deskundigen te vatten en correct weer te geven.

De zogenoemde defence (attorney's) fallacy is als het ware het spiegelbeeld. Broeders noemt het voorbeeld dat wanneer op basis van een DNA-profiel nog 2500 mannen als mogelijke dader in aanmerking komen, de kans dat zijn cliënt de dader is 1 op 2500 (0,04%) is en de kans dat zijn cliënt het niet is dus 99, 96%.[176] In dat geval berekent men de kans dat een verdachte de donor is van het gevonden spoor op basis van een eenvoudig kansmodel dat uitgaat van het totale aantal personen dat het spoor gemaakt kan hebben. De advocaat laat in deze gevallen veelal na om duidelijk te maken dat de stelling een aantal aannamen veronderstelt die niet worden genoemd. Bijvoorbeeld door aan te nemen dat alle personen een even grote kans hebben om de dader te zijn. Iedereen wordt dan even zwaar meegeteld, ongeacht leeftijd of bijvoorbeeld het hebben van een internetaansluiting.[177]

Deze valkuilen doen zich niet alleen voor bij getalsmatige uitdrukkingen, maar ook bij verbale uitdrukkingen.[178] Waar het in de kern om gaat is dat er een fout wordt gemaakt in de redenering bij de voorwaardelijke kansen of conditionele waarschijnlijkheden in de type formuleringen: 'als...dan...'. Bij de uitleg speelt ook het taalgebruik een rol. Dat een getal statistisch gezien extreem laag is, heeft bijvoorbeeld niet automatisch tot gevolg dat er geen andere oorzaken kunnen zijn dan dat de gedaagde of verdachte schuldig is. Er kan immers

[173] Broeders 2003 (diss.), p. 250.
[174] Anders gezegd de kans op een overeenkomstig DNA-profiel gegeven het feit dat het bloed niet van de verdachte is kan niet gelijk worden gesteld aan de kans dat het bloed niet van de verdachte is gegeven de overeenkomst.
[175] Taverne e.a. 2013.
[176] Broeders 2003 (diss.), p. 258.
[177] Broeders (2003) wijst erop dat de advocaat ten onrechte uitgaat van een gelijke a-priorikans voor alle 2500 personen met hetzelfde profiel, maar dat in veel gevallen de verdachte op grond van ander bewijs de status van verdachte heeft bereikt terwijl dat voor de overige 2499 niet geldt en die aanwijzingen bijdragen aan een verhoging van de a-priorikans en daarmee aan de a-posteriorkans waarin het DNA-bewijs is verdisconteerd (p. 258). Zie ook Sjerps 2008, p. 485.
[178] Sjerps 2008, p. 484.

ook sprake zijn van toeval. De kans dat iemand de staatsloterij wint is statistisch extreem klein en toch winnen mensen soms de hoofdprijs.[179]

Uit de voorgaande onderzoeken mag overigens niet worden geconcludeerd dat deze valkuilen enkel voor juristen zouden opgaan. Ook statistici geven desgevraagd aan dat de hier genoemde valkuilen kunnen optreden.[180] Schriftelijke rapportages hebben als voordeel dat het ook de expert de mogelijkheid geeft om zelf zijn verhaal nogmaals te controleren of zijn conclusies aan iemand anders voor te leggen.

Om deze valkuilen te vermijden wordt vanuit verschillende disciplines aandacht gevraagd voor de alternatieve hypothese en het aanbrengen van structuur (protocollen).[181] Daarnaast is een meer wetenschappelijke benadering van bewijs in Nederland duidelijk in opkomst. Dat blijkt niet alleen uit een toename in wetenschappelijk onderzoek en bijbehorende literatuur maar ook uit aan de specifieke opleidingen voor het OM en de rechterlijke macht.[182] In disciplines wordt aan modellen gewerkt om deze valkuilen te vermijden en ook aandacht te hebben voor alternatieve hypothesen.[183] De cursussen en onderzoeken hebben voornamelijk als doel bewustwording bij rechters te ontwikkelen die hen in staat moeten stellen hun intuïtie te controleren met expliciete rationele overwegingen.[184] Voorlopig blijft het lastig om voor de gesignaleerde valkuilen oplossingen te bedenken en deze te operationaliseren.[185] Juristen zullen zich in de regel daarom sneller aangetrokken voelen tot een maatstaf zoals de Bock deze in woorden formuleert dan in een wiskundige model zoals de Bayesiaanse methode. Daarvoor is ook in praktische zin veel te zeggen omdat een verkeerde toepassing van een in beginsel mogelijk beter model, ook tot een verkeerde uitspraak kan leiden. Wanneer de rechter zich niet bewust is van zijn beslisstrategie en bijhorende valkuilen bij statistische wetmatigheden kan hij ten onrechte een positief dan wel negatief oordeel vellen ten aanzien van de resultaten die een betrouwbaar watermerk biedt.

---

[179] Meulenbroek 20003, p. 262.

[180] Zo geeft ook Peter Grünwald, hoogleraar statistiek en zelflerende computer systemen bij het Centrum Wiskunde & Informatica, aan tijdens het Congres 'Waarheidsvinding: een juridisch doolhof?' te Leiden op 18 november 2011. Zie ook Sjerps 2005 en Broeders 2010 A, p. 5 die voorbeelden geeft van denkfouten van Van Koppen in zijn publicaties waarin hij zijn lezers juist probeert te behoeden voor deze valkuilen. Zie in de juridische literatuur Rozemond 2010.

[181] Zie over tunnelvissie en de aandacht voor tegenspraak o.m. Posthumus 2005, p. 167; Boorsma 2005; Crombag 2006; Rassin 2007; Giard 2008; Couvreur & Rassin 2010; Rassin 2010 en de reactie daarop van Aben 2011 en de reactie daarop van Rassin 2011; Giard 2011. Een van de belangrijkste uitkomsten van het rapport Posthumus 2005 naar de Schiedammer Parkmoord is dat er te weinig aandacht is geweest voor een andere verklaring voor hetzelfde feitencomplex (alternatieve hypothese).

[182] Zie ook NWO 'forensic program', waarin verschillende onderzoeken zijn toegewezen die een bijdrage kunnen leveren aan het vermijden van valkuilen.

[183] Zie voetnoot 148 voor de drie hoofdbenaderingen.

[184] Zie Rachlinski 2012.

[185] Zie ook Rassin 2012 (p. 13) die van Rachlinski 2012 meer aandacht had verwacht voor de remedies voor de geschetste problemen. Rassin ziet die in protocollen ter vergroting van de transparantie van rechterlijke beslissingen, omdat hij onder verwijzing naar Tavris & Aronson 2011 samenwerking met kritische collega's als de beste kans ziet om de gesignaleerde problemen te compenseren.

Tot slot kan nog gewezen worden op psychologisch onderzoek dat laat zien dat ook bij forensisch onderzoek de verwachtingen die men heeft over een gebeurtenis van grote invloed kunnen zijn op de waarneming en beoordeling.[186] Bij de introductie van nieuwe technieken, zoals watermerken, zijn de verwachtingen vaak hooggespannen terwijl het in de praktijk maar de vraag is of deze technieken aan specifieke vragen kunnen voldoen.[187] Watermerken zullen, evenals DNA-bewijs, geen 'truthmachine' kunnen bieden.[188] Om aan deze verwachtingen een tegenwicht te bieden is een kritische houding van alle partijen ten aanzien van de validiteit en betrouwbaarheid van een nieuwe technologie noodzakelijk. Een gebrek aan een kritische houding kan al snel leiden tot een absoluut geloof in de techniek, terwijl forensische testen nooit leiden tot absolute zekerheid maar tot wetenschappelijke uitspraken over waarschijnlijkheid.[189] Onderzoek onder Amerikaanse rechters en advocaten wijst uit dat advocaten weinig aandacht hebben voor de (technische) betrouwbaarheid van digitaal bewijs.[190] In hoeverre dat ook in Nederland het geval is, is onbekend.[191]

6.5 Het gebruik van statistiek en deskundigen in het recht

In de voorgaande hoofdstukken en paragrafen is duidelijk geworden dat de rapportage over watermerken en inbreng van experts en deskundigen een belangrijke rol spelen bij de rechterlijke waardering van het watermerk als bewijsmiddel. De rechter ziet zich bij watermerken zowel in civiele als in strafzaken in ieder geval geconfronteerd met de rapportage van de rechthebbende. Afhankelijk van het verloop van de procedure brengen partijen nog meer experts in de procedure of benoemt de rechter zelf een deskundige om vragen te beantwoorden in zaken waarover nog onduidelijkheid bestaat.

Het is uiteindelijk de rechter die het watermerk moet waarderen. Om tot die waardering te kunnen komen moet de rechter zich een oordeel kunnen vormen over de ingebrachte bevindingen van experts, kunnen vertrouwen op de expertise van de door hem benoemde deskundige en moet hij in staat zijn de inbreng van experts en deskundigen te vertalen naar een antwoord op de vraag of het watermerk een betrouwbaar bewijsmiddel kan vormen.

Het gebruik van statistisch bewijs werd in het civiel recht in Nederland door de Hoge Raad voor het eerst expliciet toegestaan in het arrest Binderen/Kaya.[192] De strafrechtzaak inzake

[186] Broeders 2003 (diss.), p. 135; Van Koppen 2011, p. 130.
[187] Zie voor de relatieve nieuwheid en veelbelovenheid van watermerken par. 3.2.1 (histgesch).
[188] Tooms 2010, p. 181 onder verwijzing naar Lynch et al 2008.
[189] Zie ook voor de paradigmawisseling van zekerheid naar waarschijnlijkheid Broeders 2002, 2005, Toom 2009, p. 417. Zie ook recent het grootschalig DNA-verwantschapsonderzoek in de zaak Vaatstra waarbij in de media al snel werd gesproken van een 100% DNA-match terwijl het NFI nooit op deze wijze resultaten naar buiten brengt.
[190] Kessler 2010.
[191] Digitaal forensische experts laten in gesprekken weten wel steeds vaker benaderd te worden om commentaar te geven op uitgevoerde onderzoeken maar geven tegelijk aan niet te weten wat er met deze informatie gebeurt.
[192] HR 10 december 1982, NJ 1983, 687, m.nt. EAA (Binderen/Kaya), ov. 4.1. Zie verder o.m. HR 25 juni 1993, NJ 1993/686, m.nt. PAS; HR 9 oktober 1992, NJ 1994/535, m.nt. CJHB; HR 6 april 1990, NJ 1990/573, m.nt. PAS; HR 7 maart 1980, NJ 1980/365.

Lucia de B. geldt als een van de bekendste zaken waarin statistiek een belangrijke rol speelde bij het bewijs en waarin later een gerechtelijke dwaling werd vastgesteld. Deze zaak geeft een goed beeld van de problemen waarvoor de rechter zich gesteld ziet. Aan de hand van de zaak Lucia de B. zal duidelijk worden gemaakt dat het gebruik van statistiek als bewijs niet zonder risico is voor de waarheidsvinding en daarmee voor het watermerk als bewijsmiddel. Voor de bespreking van deze zaak wordt specifiek aandacht besteed aan de zogeheten rechterlijke dwalingen die rechtstreeks verband houden met het gebruik van statistiek.[193]

In de zaak Lucia de B. draait het om een verpleegster die tijdens haar diensten bij twee ziekenhuizen een ogenschijnlijk groot aantal incidenten meemaakt waarna er door de directeur van één van deze ziekenhuizen aangifte wordt gedaan. Bij de rechtbank 's-Gravenhage staat in 2003 naast de medische vragen naar de doodsoorzaak de vraag centraal hoe groot de kans is dat zij per toeval betrokken is bij deze incidenten.[194] Het OM wilde weten hoe groot de kans was dat een verpleegkundige bij toeval evenveel incidenten in de twee ziekenhuizen zou meemaken. Daarvoor maakte het OM gebruik van de deskundigheid van dr. H. Elffers die, zoals in de statistiek gebruikelijk is, een model gebruikt, de situatie beschrijft en hypothesen formuleert die hij vervolgens toetst. Meester, die later als deskundige voor de verdediging optreedt, beschrijft het model van Elffers bij een bespreking van deze zaak als volgt: 'als we de hypothese hanteren dat Lucia de B. onschuldig is, dan zal gedurende een dienst van haar de kans op een incident niet groter zijn dan tijdens elke andere willekeurige dienst.'[195] Dat zou betekenen dat de incidenten volkomen willekeurig verspreid zullen liggen over alle diensten in het ziekenhuis en dat berekend kan worden wat de kans is dat wanneer alle incidenten toevallig aan bepaalde diensten worden toegewezen Lucia de B. tenminste evenveel incidenten mee zou maken als in werkelijkheid het geval is.[196] Elffers rapporteerde daarover dat de kans dat een verpleegkundige bij toeval net zoveel incidenten in de twee ziekenhuizen mee zou maken als verdachte 1 op de 342 miljoen bedraagt.[197] De aard en inhoud van deze rapportage is voor de rechtbank aanleiding om ambtshalve prof. mr. R.V. de Mulder te benoemen als deskundige. De rechtbank volgt hem in zijn verklaring dat het onderzoek in uitgangspunten, de gevolgde berekeningsmethode en gevonden uitkomsten vanuit wetenschappelijk oogpunt correct is. Op grond daarvan komt de rechtbank tot het oordeel dat het uitermate onwaarschijnlijk moet worden geacht dat verdachte de in de tenlastlegging genoemde incidenten in het JKZ en RKZ bij toeval heeft meegemaakt.[198] De rechtbank benadrukt echter dat hier niet zonder meer uit kan worden afgeleid dat verdachte deze incidenten ook heeft veroorzaakt. Daarbij maakt het duidelijk dat de uitkomsten van statistische berekeningen op zichzelf beschouwd geen wettig en overtuigend bewijs voor dit laatste opleveren maar ook niet betekenen dat zij in het geheel niet kunnen bijdragen tot de

[193] In deze zaak komen vanzelfsprekend ook de medische aspecten rondom de doodsoorzaak van de patiënten aan de orde. In de kern genomen gaat het in deze zaak echter fout bij het gebruik van statistiek.
[194] Rb. 's-Gravenhage 24 maart 2003, ECLI:NL:RBSGR:2003:AF6172 (Lucia de B.).
[195] Statistiek en kansrekening in het strafrecht, Ronald Meester*, AA 2007, p. 675
[196] Door het geobserveerde aantal incidenten willekeurig over alle diensten te verdelen.
[197] Rb. 's-Gravenhage 24 maart 2003, ECLI:NL:RBSGR:2003:AF6172 (Lucia de B.), ov. 7. Los van het gebruikte model is er door statistici ook gewezen op de rekenfouten die Elffers gemaakt zou hebben.
[198] Rb. 's-Gravenhage 24 maart 2003, ECLI:NL:RBSGR:2003:AF6172 (Lucia de B.), ov. 11.

bewijsvoering. De rechtbank volgt daarin het Hof Amsterdam dat eerder cumulatief drie voorwaarden had opgesteld.[199] Zo stelde de rechtbank vast dat (1) buiten redelijke twijfel moet staan dat voor het statistische verband tussen verdachte en de op de tenlastlegging genoemde ernstige incidenten, geen alternatieve verklaring bestaat; (2) voorts buiten redelijke twijfel moet staan dat het ernstige incident bij de betreffende patiënt niet verklaard kan worden door een buiten verdachte gelegen medische oorzaak; (3) en dat in deze zaak ook concrete andere bewijsmiddelen voorhanden moeten zijn die wijzen op een causaal verband tussen verdachte en het zich voordoen van ernstige incidenten. Deze laatste twee criteria dragen ertoe bij dat de rechtbank niet in alle gevallen de feiten bewezen acht. Maar alleen in die gevallen waarin geen andere medische oorzaak het incident kan verklaren en er concreet ander bewijs aanwezig was.

In hoger beroep maakt de verdediging gebruik van de deskundigheid van R. Meester als getuige-deskundige.[200] Hij maakt duidelijk dat het getal zelf in beginsel betekenisloos is omdat het afhangt van verschillende onderliggende aannames en bovendien bewijst een klein getal niet dat het niet om toeval kan gaan. Ter zitting wordt hem gevraagd wat de kans dan wel is. Wanneer Meester hierop antwoordt dat in dit geval niet op een zinvolle manier een relevante kans bepaald kan worden, wordt hem nogmaals gevraagd, wat volgens hem de kans is. Het hof maakt duidelijk dat in tegenstelling tot de rechtbank de berekeningen van Elffers geen expliciete rol spelen bij het bewijs door dit in het arrest op te nemen: ‘Er is geen statistisch bewijs in de vorm van toevalsberekeningen gebruikt.'[201] Hoewel het hof inderdaad geen blijk geeft van het gebruik van berekeningen kan niet worden gezegd dat het hof geen gebruik maakt van kansberekening. Statistici wijzen erop dat in het arrest van het hof weliswaar geen berekeningen worden aangetroffen, maar dat het hof wel gebruik maakt van toevalsredeneringen om tot een bewezen verklaring te komen.[202] Bovendien kan niet worden uitgesloten dat de uitkomsten en het oordeel van de deskundige een rol hebben gespeeld bij de overtuigingsvorming (conviction intime).

De zaak wordt in eerste instantie nog gecasseerd vanwege de ontoelaatbare combinatie in de strafoplegging van levenslang en TBS, maar zij wordt door het hof alsnog tot levenslang veroordeeld.[203] Daarna krijgt de zaak onder meer door het boek ‘Lucia de B.: reconstructie van een gerechtelijke dwaling’ van prof. T. Derksen de aandacht van de Toegangscommisie Evaluatie Afgesloten Strafzaken (CAES) die uiteindelijk echter onvoldoende grond voor een herziening ziet. Het eigen onderzoek van A-G Knigge vanwege een onvoldoende inhoudelijk oordeel over het geconstateerde verschil van wetenschappelijk inzicht in de bevindingen van

[199] Hof Amsterdam 7 oktober 2003 ECLI:NL:GHAMS:2003:AL7736, ov. 5.
[200] Hof ‘s-Gravenhage 18 juni 2004, ECLI:NL:GHSGR:2004:AP2846 (Lucia de B.).
[201] Idem.
[202] Grunwald 2011 http://www.luciadeb.nl/metta/Grunwalds-Metta-analyse.pdf; Colignatus 2007: http://www.math.leidenuniv.nl/~gill/2007-06-26-Colignatus-Ldb-HE-RdM.pdf
[203] HR 14 maart 2006, ECLI:NL:HR:2006:AU5496, NJ 2007, 345, m.nt. P.A.M. Mevis; Hof Amsterdam 13 juli 2006, ECLI:NL:GHAMS:2006:AY3864 (Lucia de B.).

het CAES leidt tot een herziening bij de Hoge Raad en uiteindelijk tot vrijspraak door het hof.[204]

In de literatuur is deze zaak uitgebreid besproken, zowel onder juristen als onder statistici.[205] Voor meer inhoudelijke overwegingen ten aanzien van statistiek in het recht verwijs ik naar de literatuur.[206] Voor het gebruik van watermerken is de zaak Lucia de B. in een aantal opzichten relevant.

Deze zaak laat ten eerste zien dat ondanks de poging van de wetgever om de beslissing van de rechter te kanaliseren fouten heel goed mogelijk zijn.[207] De rechter in eerste aanleg heeft in deze zaak binnen de kaders van het bewijsrecht en de motiveringsplicht zijn uiterste best gedaan. Hij heeft niet alleen de partij-deskundige gehoord (Elffers) maar ook zelf een deskundige (De Mulder) aangesteld om de partij-deskundige te controleren. Daarnaast heeft hij in het eindvonnis uitgebreid stilgestaan bij de motivering van het vonnis. Hetzelfde geldt voor het hof, zij het dat het hof naar mijn mening ongelukkig is in de uitwerking van zijn arrest door duidelijk te maken dat statistiek geen rol meer speelt, maar tegelijk in zijn redenering wel gebruik maakt van kansberekeningen. Deze zaak maakt duidelijk dat verantwoording en controle mogelijk zijn, maar de kwaliteit van de overtuiging het pijnpunt vormt.[208] Omdat de rechter mede vanwege efficiencyredenen niet in hoeft te gaan op alle bewijsmiddelen wordt niet altijd duidelijk waarom het ene bewijsmiddel wel wordt gebruikt ter verificatie of verankering en het andere niet ter falsificatie.[209] Dit probleem is volgens Buruma niet op te lossen door snel te grijpen naar 'in dubio pro reo'. Hij wijst tevens op de inmiddels aangescherpte motiveringsplicht.[210] Het is tevens een open vraag of een uitgebreidere motiveringsplicht helpt, omdat de sprong die de rechter maakt ongrijpbaar is. Uiteindelijk worden de bewijsmiddelen die niet met zijn overtuiging overeenstemmen weggeschreven.[211] Soms is dat terecht en soms onterecht.

Ten tweede is deze zaak bijzonder omdat in tegenstelling tot andere rechterlijke dwalingen zoals de Schiedammer Parkmoord, in deze zaak voldoende tegenspraak is geweest (ook reeds bij politie en OM) en niet kan worden gesproken van een 'confirmation bias' (of

[204] Geen herziening CAES (23-11-2007), eigen onderzoek A-G Knigge leidt tot herziening door de Hoge Raad op 7 oktober 2008, ECLI:NL:HR:2008:BD4153, NJ 2009, 44 m.nt. P.A.M. Mevis; Hof Arnhem 14 april 2010, ECLI:NL:GHARN:2010:BM0876, NJ 2010, 363 m. nt. P.A.M. Mevis (Vrijspraak Lucia de B.). Zie voor een chronologische volgorde en alle instanties het dossier op rechtspraak.nl.
[205] Zie door juristen o.m. Buruma 2010 en door statistici o.m. Lambalgen & Meester 2004, Van Zwet 2004 en de reactie daarop van Elffers 2003, Elffers 2004b. Zie ook Sjerps & Coster van Voorhout 2005 en de daar aangehaalde literatuur.
[206] Zie o.m. Het themanummer over 'Statistiek in de rechtszaal' in Stator jrg 5, nr. 2, juni 2004; Nijboer 2004; Sjerps & Coster van Voorhout 2005; Meester 2007
[207] Zie voor dat kader de vorige paragrafen waarin het bewijsrecht en de motiveringsplicht zijn besproken.
[208] Zie Buruma 2010, p. 702; vgl. Telders 1937 en Nieuwenhuis (1976) die voor het civiele recht al kort gezegd duidelijk maakte dat beslissen en motiveren twee verschillende zaken zijn.
[209] Zie ook Buruma 2010, p. 702.
[210] Buruma (2010, p. 701) wijst o.m. art. 359 lid 2 Sv; de toename van motivering en bereidheid daartoe en de impact van de Schiedammer Parkmoord.
[211] Zie o.m. Visser 2008.

tunnelvisie).[212] In plaats daarvan leidde, zoals Buruma het beschrijft, 'een cascade aan fouten' tot de onterechte veroordeling van Lucia de B.[213] Buruma concludeert dan ook terecht dat er in juridische zin en in termen van rechtzetting weinig aan te merken valt op het gehele proces van Lucia de B. Tegenspraak blijft van groot belang evenals de waakzaamheid van de rechter voor een werkwijze die hem bij de selectie en waardering ontvankelijk maakt voor overtuigende kracht van een cascade van onvoldoende precies uitgezochte indicaties.[214] De gedaagde of verdachte zal om die reden zelf ook voldoende aandacht moeten hebben voor een kritische benadering van het watermerk om daarmee de rechter te helpen waakzaam en kritisch te blijven.

Ten derde laat deze zaak zien dat voor de keuze van een deskundige in sommige situaties al een behoorlijke mate van deskundigheid is vereist. Een van de problemen bij de keuze van de deskundige is dat de vraag die rechters beantwoord willen zien, bij het benoemen van de deskundige, al duidelijk moet zijn. Dat de vraagstelling van belang is laat Rassin zien in een voorbeeld.[215] Wie geïnteresseerd is in de oorzaken van criminaliteit zal snel in de literatuur terechtkomen over sociale processen, disfunctionele leergeschiedenis, overvloed aan testosteron, (nor)adrenaline en wellicht psychopathie en antisociale persoonlijkheidsstoornis. De (gespiegelde) vraag waarom sommige mensen zich niet aan de regels houden komt in andere literatuur terecht, bijvoorbeeld die over serotonine, problemen met inhibitie en delay of gratification. De wijze waarop de vraag of opdracht door de rechter is geformuleerd is daarmee van invloed op de vraag wie als deskundige moet worden benoemd. Uit het vonnis in de zaak Lucia de B. blijkt niet waarom de rechter De Mulder als deskundige heeft gevraagd. Mogelijk is dat gelegen in het feit dat hij eenmaal een artikel heeft gepubliceerd in het NJB over statistiek en bewijsrecht.[216] Dat hij geen deskundige is op dit terrein van de statistiek wordt duidelijk wanneer twee hoogleraren uit andere disciplines de verklaring, dat de mogelijkheid dat de verdachte vaker relatief ernstig zieke patiënten verzorgde, de uitkomsten van de waarschijnlijkheidsberekeningen niet wezenlijk zou beïnvloeden, onbegrijpelijk vinden.[217] Vanwege de vertaalslag tussen de jurist en de voorliggende statistische vraag is de keuze niet onlogisch. Het was echter beter geweest om deze deskundige te vragen om de vraag te vertalen en daarbij zelf een lijst met deskundigen voor te stellen. Daarbij kan ook gewezen worden op de rol van de deskundige zelf die zijn eigen deskundigheid niet had moeten overschatten. Om een totaaloordeel te kunnen geven over onderdelen van een watermerksysteem of de betrouwbaarheid van een systeem zal de rechter aansluiting moeten zoeken bij een deskundige die zowel ervaring heeft in het domein van forensisch onderzoek als in het domein van watermerken. De rechter zou er vanwege de transparantie goed aan doen om te onderbouwen op welke gronden hij besloten heeft om de door hem benoemde

[212] Zie ook Buruma 2010, p. 695.
[213] Deze cascade ontstond volgens Buruma (2010, p. 697) doordat teveel tegensprekers niet zuiver beargumenteerden en een groep vormden waarbinnen 'een explosieve mix van technisch-wetenschappelijke argumenten, vertrouwen in gezaghebbende deskundigen en emotionele besmetting tot stand kwam'.
[214] Buruma 2010, p. 706.
[215] Rassin 2012, p. 14.
[216] Kermeester & e Mulder, 'Statistiek en bewijsrecht', NJB 1987, p. 73-81.
[217] Van Lambalgen & Meester 2004.

deskundige te benoemen. De gedaagde of verdachte kan de rechter helpen in dit proces door zelf een deskundige voor te stellen dan wel kritisch te zijn op de aan te stellen deskundige.[218]

Ten vierde kan de inbreng van het wetenschappelijk forum en andere statistici worden genoemd. Deze zaak is niet alleen door juristen besproken in verschillende publicaties maar ook uitvoerig door statistici zelf waardoor het eenvoudig mogelijk was om gebreken die samenhingen met de uitleg en het gebruik van statistiek kenbaar te maken. De inbreng van deze groep heeft er mede aan bijgedragen dat 'fouten' uiteindelijk hersteld konden worden. Mogelijk ligt in dit laatste punt ook de oplossing ten aanzien van meer digitaal forensisch bewijs. Eerder is duidelijk geworden dat de inbreng van experts veelal nodig zal zijn in zaken waarin technisch bewijs een doorslaggevende of belangrijke rol speelt.[219] Zowel in het civiel als in het strafrecht zullen beide partijen de inbreng van experts nodig hebben om te voorkomen dat de rechter (te) snel tot een oordeel komt ten aanzien van het technisch bewijs.

Een belangrijk aspect bij de inbreng van experts zijn de kosten die daarmee gepaard gaan. Daarnaast kan naar aanleiding van de zaak van Lucia de B. er ook op worden gewezen dat andere fora nuttig kunnen zijn bij het vaststellen van de waarheid. Niet in de laatste plaats omdat een storm aan kritiek een indicatie kan zijn dat er fouten zijn gemaakt bij het beoordelen van bepaalde zaken. In die zin kan met name in hoger beroep voordeel worden getrokken uit het feit dat rechters in een zaak in eerste aanleg voldoende motiveren waarom de ene expert of deskundige moet worden gevolgd en de andere niet.[220] Die informatie geeft mensen de mogelijkheid om te reageren en fouten van zowel de expert of deskundige zelf te bekritiseren alsmede onjuiste gevolgtrekkingen die de rechter zelf heeft gemaakt naar aanleiding van de inbreng van experts of deskundigen. Dit laatste vereist ook openbaarheid van de stukken waarop zaken zijn gebaseerd. Er zou zeker ten aanzien van digitaal forensisch bewijs, en voor dit onderwerp watermerken in het bijzonder, opnieuw nagedacht moeten worden over de vraag in hoeverre stukken openbaar beschikbaar moeten kunnen komen. Met name bij digitaal forensisch bewijs zijn er mogelijk voldoende mensen bereid om mee te denken of bepaalde fouten in onderzoeken te ontdekken. Of juist te bevestigen dat de resultaten uit het onderzoek aannemelijk zijn. Zo kan het gebrek aan een hackspoor in een zaak een belangrijk gegeven zijn, terwijl iemand op een forum zou kunnen toegeven dat er wel degelijk een hack heeft plaatsgevonden. Informatie ten aanzien van die hack kan ertoe leiden dat de expert of deskundige de kans dat een bepaald feit zich heeft voorgedaan anders inschat.[221] Ook voor het op de juiste wijze beoordelen van watermerken kan de inbreng van het wetenschappelijk forum en andere statistici uiteindelijk van groot belang zijn.

[218] Zie par. 6.2.2.
[219] Zie hoofdstuk 4 waarin duidelijk werd dat in civiele zaken de eiser veelal een verslag van een expert nodig heeft om relatief nieuwe technische middelen als bewijs te kunnen gebruiken en de gedaagde een experts nodig is om dat bewijs voldoende te kunnen betwisten.
[220] Zie ook Den Tonkelaar 2015, p. 598, die stelt dat het zeer de moeite waard kan zijn om een inhoudelijk verschil van mening (tussen rechters in raadkamer) aan te geven in de uitspraak.
[221] Zie hoofdstuk 4, par. 4.2.2 en par. 4.4.2.

Om fouten in hoger beroep te kunnen herstellen zouden rechters de resultaten van expert- of deskundigenonderzoek inhoudelijk uitgebreider moeten motiveren en zouden de rapporten geanonimiseerd toegankelijk moeten worden waardoor controle door (andere) experts mogelijk wordt.[222] Het belang daarvan werd duidelijk in de zaak van Lucia de B. Een andere mogelijkheid zou kunnen zijn de deskundige de mogelijkheid te bieden een dissenting opinion te schrijven wanneer hij inhoudelijk van mening is dat de rechter een bepaalde gevolgtrekking ten aanzien van het bewijs niet kan trekken. Het is dan vervolgens aan partijen om te bepalen of die informatie, mede in het licht van de zaak, van voldoende belang is om hoger beroep in stellen.

Buruma wijst er na de vrijspraak van Lucia de B. op dat de boodschap van deze zaak niet is 'dat we met zijn allen geen spijt hoeven te hebben, maar slechts deernis met de vrouw die tussen de raderen van het systeem belandde'.[223] Hij wijst er verder op dat de boodschap is dat het alert inschakelen van de autoriteiten niet altijd goed is, tegenspraak ook een koor kan opleveren dat ons in slaap sust, gedetineerden en bewakers zich bewust moeten zijn van de lotsverbondenheid met elkaar en dat de feitenrechter zich inderdaad moet hoeden voor een werkwijze bij de selectie en waardering van de feiten die hem ontvankelijk maakt voor de overtuigende kracht van een cascade van onvoldoende precies uitgezochte indicaties. En dat zijn volgens Buruma ongemakkelijke lessen. Of en wat het recht daaraan kan doen laat hij vervolgens onbesproken. De hiervoor genoemde punten betreffen echter geen zaken die direct (proces)recht raken. Het (proces)recht laat de waardering van het bewijs immers aan de rechter over.[224] Ingrijpen in het procesrecht ten aanzien van de waardering door de rechter zal niet snel worden aangenomen. Van de vier door Buruma genoemde boodschappen raken er twee direct de waardering van het bewijs, namelijk de boodschap dat tegenspraak ook een koor oplevert dat ons in slaap sust en dat de feitenrechter zich inderdaad moet hoeden voor een werkwijze bij de selectie en waardering van de feiten die hem ontvankelijk maakt voor de overtuigende kracht van een cascade van onvoldoende precies uitgezochte indicaties. In beide gevallen gaat het om een oproep aan de rechters om waakzaam te zijn. Het is eenvoudiger om te constateren dat de rechters waakzaam moeten zijn dan om met suggesties te komen hoe de rechters dat zouden moeten bewerkstellingen. Het probleem dat zich hier voordoet is hiervoor al eerder benoemd en komt neer op het stellen van de juiste vraag en vervolgens van de juiste onderzoeksrichting. Van besliskunde en psychologie heb ik te weinig kennis zodat ik mij op die gebieden niet moet willen begeven. De door Buruma genoemde boodschappen komen er uiteindelijk op neer dat rechters meer training nodig hebben om beter voorbereid de steeds complexer wordende zaken tegemoet te treden. Waakzame rechters moeten niet alleen tijd hebben om vakkennis bij te houden, dossiers te bestuderen en inhoudelijk goed getraind zijn om de juridisch kennis te kunnen toepassen maar ook waakzaam zijn ten aanzien van verschillende andere processen die spelen bij het nemen van soms complexe beslissingen. Dat betekent ook dat rechters voldoende tijd moeten hebben om tot een goede beslissing te

[222] Zie ten aanzien van het geanonimiseerde rapport, ook Broeders 2010 B, p. 113.
[223] Buruma 2010, p. 706.
[224] Dat geldt zowel voor het Nederlandse als Belgische civiel en strafprocesrecht. Zie daarvoor hoofdstuk 4.

komen.[225] Dat geldt ook bij het waarderen van watermerken als juridisch bewijsmiddel. Uiteindelijk stelt het beleidsmakers, maar ook de samenleving voor de vraag hoeveel tijd en geld een procedure mag kosten. En dat zijn vragen die in beginsel buiten het domein van het recht zelf vallen, maar wel van invloed zijn op de toepassing en uitvoering van het recht.

Evenals bij wetenschap geldt ook voor de rechterlijke macht dat 'Trial and Error' de motor is van vooruitgang. De rechter zit aan het einde van een heel traject, waarin zich op verschillende momenten en niveau's problemen voor kunnen doen. Daar ligt een taak voor de wetenschap om handvatten aan te reiken, maar mogelijk ook om enkele instituten opnieuw in overweging te nemen. Vooralsnog is er weinig reden de waardering van het bewijs door rechters aan juridische banden te leggen. De belangrijkste conclusie is, zoals Groenhuijsen signaleerde in zijn artikel over de aanval van deskundigen op de kwaliteit in de strafrechtspleging, dat er verschillende disciplines samenwerken om die kwaliteit te verbeteren.[226] Inmiddels zijn er verschillende (multidisciplinaire) onderzoeken gestart om bruggen te kunnen slaan en rechters mogelijk hulpmiddelen te bieden die de kans op fouten in de toekomst zo klein mogelijk maken.[227] Deze hulpmiddelen moeten de rechter ook meer houvast geven bij het beoordelen van watermerken als juridisch bewijsmiddel. De zaak Lucia de B. heeft namelijk laten zien dat voor de waarheidsvinding voor alle partijen een rol is weggelegd. De rechthebbende moet kritisch op zijn eigen forensische proces en naar de leverancier van watermerken om ervoor te zorgen dat de kans op fouten minimaal is. De gedaagde zal kritisch moeten zijn op de aangeleverde rapportage en bij het aanstellen van een eventuele deskundige door de rechter. De rechter zal tot slot bij zijn beoordeling waakzaam moeten zijn dat hij geen werkwijze hanteert die hem bij de selectie en waardering ontvankelijk maakt voor overtuigende kracht van een cascade van onvoldoende precies uitgezochte indicaties. Bij het benoemen van een deskundige zal hij er rekening mee moeten houden dat hij een deskundige aanstelt die zowel ervaring heeft in het domein van forensisch onderzoek als in het domein van watermerken. De rechter zou er vanwege de transparantie tevens goed aan doen om te onderbouwen op welke gronden hij besloten heeft om de door hem benoemde deskundige te benoemen. Tot slot zou de uitspraak het mogelijk moeten maken dat het wetenschappelijk forum en andere statistici in staat worden gesteld om gebreken die samenhangen met de uitleg en het gebruik van statistiek bij watermerken kenbaar te maken. Daarvoor is vereist dat voldoende relevante informatie in de uitspraak is opgenomen. Op deze manier kan de inbreng van deze groep eraan bijgedragen dat 'fouten' uiteindelijk kunnen worden hersteld.

[225] Zie tegen die achtergrond ook het manifest dat rechters presenteerde (Opiniepagina NRC, 4 februari 2013).
[226] Groenhuijsen 2008 p. 941.
[227] Zie onder meer het in 2012 begonnen multidisciplinaire (informatica, chemie en wiskunde) NWO-programma forensic science dat ten doel heeft wetenschappelijke onderbouwing te bieden, risico te verminderen en de betrouwbaarheid van forensisch onderzoek te vergroten.

6.6 Samenvatting en conclusie

In dit hoofdstuk is de waardering van het watermerk behandeld. Voor de waardering van het watermerk is gekeken naar de betrouwbaarheid van het gehele proces van watermerken, van het aanbrengen van de juiste gegevens tot het interpreteren ervan. De betrouwbaarheid van het watermerk als bewijsmiddel ziet op authenticatie van personen, en het watermerk zelf.

De betrouwbaarheid van watermerken speelt in het civiele proces een andere rol dan in het strafrecht. In het civiele recht geldt als uitgangspunt dat het watermerk een betrouwbaar bewijsmiddel is, tenzij de gedaagde daar verweer tegen voert. Wanneer de gedaagde dit niet of onvoldoende doet dan kan de rechter het feit vaststellen. Dit geldt ook in het geval dat het watermerk als bewijsmiddel objectief gezien geheel onbetrouwbaar is. De civiele rechter komt in beginsel enkel toe aan de beoordeling van de betrouwbaarheid van watermerken als partijen daar in stellingen aanleiding toe geven. De strafrechter heeft in theorie meer ruimte om zelf de betrouwbaarheid te onderzoeken, maar het is de vraag in hoeverre de rechter de betrouwbaarheid van het bewijsmiddel ook daadwerkelijk onderzoekt.

Het watermerk wordt in beide landen en rechtsgebieden in de regel gepresenteerd in de vorm van een rapportage of verslag. Om te beoordelen of het watermerk een betrouwbaar bewijsmiddel is, is in dit hoofdstuk onderzocht wanneer de rechter aan de rapportage van de rechthebbende voldoende bewijskracht kan toekennen om het watermerk als bewijsmiddel te accepteren om daarmee het feit dat het bestand aan de licentienemer toebehoort vast te stellen. Om tot die vaststelling te komen spelen drie elementen een rol.

Ten eerste moet de rapportage voldoen aan de algemene eisen die gesteld worden aan (digitaal) forensisch onderzoek (par. 6.2). Om de betrouwbaarheid van watermerken vast te kunnen stellen moet naar het gehele proces van watermerken gekeken worden: van het aanbrengen van de juiste gegevens tot het op een juiste wijze interpreteren van de bevindingen. Voor de beoordeling van dit gehele proces kan aansluiting worden gezocht bij de wijze waarop forensisch onderzoek dient te worden verricht. Dat betekent dat ervoor betrouwbaar bewijs niet alleen sprake moet zijn van het gebruik van de juiste techniek gecombineerd met de juiste invoer van gegevens maar ook dat de gehele organisatie zo is ingericht dat de betrouwbaarheid ervan kan worden gegarandeerd. Dat betekent dat de organisatie in staat moet zijn het gehele proces inzichtelijk te maken en te laten controleren. De rechthebbende moet met andere woorden in staat zijn om door middel van een zogenoemde chain of custody een zogenaamde chain of evidence te maken. Bijvoorbeeld om aan te kunnen tonen dat de koppeling van de gegevens van de licentienemer en het watermerk juist is of dat het op internet aangetroffen bestand ook daadwerkelijk het bestand is waarop onderzoek is verricht en waarin het desbetreffende watermerk is gevonden. Dit proces is niet nieuw maar dient wel aandacht te krijgen bij de beoordeling van het watermerk als bewijs en bij het opstellen van het verslag. De rechthebbende zal hiermee dan ook rekening moeten houden bij het inzetten van een dergelijk systeem. Het vormt een duidelijke randvoorwaarde

voor de inzet van betrouwbare watermerken als juridisch bewijsmiddel en eventueel het inhuren van organisaties die deze dienst aanbieden. Het onvoldoende rekening houden met de wijze waarop watermerken wordt georganiseerd hoeft de betrouwbaarheid ervan niet per definitie aan te tasten. De rechthebbende neemt daarmee wel het risico dat hij later onvoldoende kan aantonen dat het watermerk betrouwbaar is en dat de rechter hierdoor ook niet overtuigd raakt dat het feit zich heeft voorgedaan.

Ten tweede moet in het verslag duidelijk worden of het watermerk een betrouwbaar bewijsmiddel is (par. 6.3). De betrouwbaarheid van het watermerk ziet in beginsel op twee aspecten. De gegevens die in het watermerk worden gestopt moeten juist zijn (authenticatie licentienemer) en het watermerken als techniek moet betrouwbaar zijn. Dat wil zeggen dat dezelfde gegevens die in het watermerk zijn gestopt er ook weer uit te halen zijn. Voor het beoordelen van het watermerk als techniek zijn op grond van de literatuur een aantal onderwerpen onderscheiden die van belang zijn voor het gebruik van watermerktechnieken en daarmee voor betrouwbare resultaten. Om het watermerk als techniek betrouwbaar te achten zal in de rapportage aandacht moeten zijn voor de wijze waarop het gehele systeem is ingericht en de wijze voor het valideren van de gebruikte techniek en processen. Daarnaast zal in het verslag duidelijk moeten worden voor welke watermerktechniek is gekozen en welke keuzes de rechthebbende heeft gemaakt, alsmede in welke mate dit de betrouwbaarheid van het onderzoek aantast. Dat betekent ook dat duidelijk zal moeten worden of de gebruikte sleutels en algoritmen betrouwbaar zijn. Hierbij zal ook duidelijk moeten worden op welke wijze de watermerken worden aangebracht en gedetecteerd. Vervolgens moet in de rapportage duidelijk worden wat de meest aannemelijke aanvallen zijn op de gekozen watermerken. En of en zo ja welk effect dat heeft op betrouwbaarheid van het watermerk als bewijsmiddel in de zaak waarin de rapportage wordt ingebracht. Tot slot zal de rechthebbende ook rekenschap moeten geven van de meest aannemelijke verweren die de gedaagde kan voeren ten aanzien van de betrouwbaarheid van het watermerk als bewijsmiddel. Bij deze verweren staat de vraag centraal onder welke omstandigheden watermerken de verkeerde uitkomst kunnen geven. In de rapportage zal om die reden aandacht moeten zijn voor de vraag hoe groot de kans is dat er fouten zijn gemaakt in het authenticatieproces (verkeerde naam), fouten bij het inzetten van de techniek van watermerken waardoor er sprake kan zijn van een fout-positief, en de kans dat iemand anders het bestand met ‘zijn’ traitor tracingscode en zonder zijn medeweten heeft verspreid (vals watermerk). En in welke verhouding deze kans moet worden begrepen. In de rapportage zal onder meer duidelijk moeten worden welke maatregelen zijn genomen om voornoemde situaties te voorkomen.

Ten derde is het van belang dat de rechter resultaten van het rapport op de juiste waarde weet te schatten (par. 6.4). Dat betekent dat de rechter aandacht moet hebben voor de valkuilen die er bestaan bij het komen tot een bewijsbeslissing, in het bijzonder ten aanzien van de invloed die getallen hebben op lezers van het rapport (par. 6.5). De rechter zal zich rekenschap moeten geven dat het lezen van een rapportage niet eenvoudig is. Evenals bij rapportages ten aanzien van DNA-bewijs zal ook bij watermerken in het verslag gebruik worden gemaakt van

verschillende kansberekeningen. Onderzoek naar DNA-bewijs wijst uit dat juristen moeite hebben met het lezen van deze verslagen. Zelfs juristen die aangaven de rapporten te begrijpen bleken vaak niet in staat om de conclusie van het rapport op een juiste wijze te beschrijven. Dit gegeven zou de rechter waakzaam moeten maken dat op zichzelf betrouwbare informatie ook tot een juiste bewijsbeslissing leidt. Een onjuiste interpretatie van de gerapporteerde onderzoeksresultaten kan immers leiden tot misvattingen over de sterkte van watermerken als bewijs. Vanuit het perspectief van de rechthebbende duiden deze onderzoeken op een risico bij het inzetten van watermerken als bewijs. Tegen deze achtergrond kunnen zelfs betrouwbare watermerken het watermerk nog ineffectief maken.

Uiteindelijk biedt watermerken evenals DNA-bewijs vooral bewijs in de vorm van een kansberekening of zeldzaamheidswaarde. De rechter bepaalt mede uiteindelijk in het licht van andere bewijsmiddelen wat de bewijswaarde is van deze kansberekening en welke rol die speelt in het totale beeld of verhaal in deze zaak. In zoverre hebben Finkelstein & Fairly (1970, p. 497) een punt wanneer zij stellen dat ‘Guilt is determined by a cumulation of probabilities’.[228]

Het voorgaande maakt duidelijk dat er bepaalde risico’s zijn ten aanzien van de waardering van het watermerk als juridisch bewijsmiddel. In de praktijk is het dan ook de vraag of het watermerk als juridisch bewijsmiddel het meest effectieve bewijs is. Evenals ander forensisch bewijs moet het een lange weg afleggen voordat het daadwerkelijk als bewijsmiddel kan worden gebruikt.

[228] Finkelstein & Fairly 1970, p. 517.

7 Over watermerken als juridisch bewijsmiddel

7.1 Inleiding

In dit onderzoek is de vraag centraal gesteld of een niet-waarneembaar digitaal watermerk dat als doel heeft de licentienemer te traceren (hierna: het watermerk), in Nederland een effectief bewijsmiddel kan vormen voor de handhaving van auteursrechten op digitaal beschikbaar gestelde foto's, muziek en video op internet.[1] Het watermerk is in dit onderzoek effectief wanneer de rechter het gestelde feit waarvoor het watermerk wordt aangevoerd bewezen kan achten. In dit onderzoek is vergelijkenderwijs naar het Belgische civiele recht en strafrecht gekeken.

Dit onderzoek naar de technische en juridische aspecten van watermerken is begonnen (2009) vanuit het idee dat rechthebbenden vanwege de eenvoudige wijze waarop digitale content kan worden gekopieerd en verspreid, terughoudend zijn met het op digitale wijze ter beschikking stellen van hun content. Destijds was recent afscheid genomen van de consument-onvriendelijke kopieerbeveiliging als een vorm van DRM, waardoor DRM als containerbegrip ten onrechte een negatieve lading had gekregen in het publieke debat. De kopieerbeveiliging heeft duidelijk gemaakt dat consumenten niet in hun (legale) handelingen gehinderd wilden worden. Digitale watermerken in dit onderzoek voldoen aan dat criterium en zijn in die zin een vorm van DRM met een vriendelijker gezicht.

In de afgelopen jaren is de techniek ook in de literatuur volwassen genoeg bevonden voor commercieel gebruik. Aanvankelijk was mijn verwachting dat watermerken mede vanwege de goede mogelijkheden om informatie te verbergen in grote bestanden zoals muziek, video en foto's zich in deze sectoren zouden ontwikkelen. Tegen het einde van dit onderzoek werd duidelijk dat watermerken in ieder geval een rol hebben gekregen in de praktijk van het beveiligen van e-boeken. Welke rol watermerken precies spelen in deze andere sectoren blijft vooralsnog onduidelijk(er).

Voor het beantwoorden van de onderzoeksvraag is eerst gekeken naar de vraag hoe het watermerk werkt en welke rol het watermerk krijgt in de watermerkliteratuur (par. 7.2). Vervolgens is aan de hand van het materiële recht (auteursrecht) gekeken naar de rol die het watermerk kan spelen bij het vaststellen van auteursrechtinbreuk (par. 7.3). Na bestudering van de watermerkliteratuur en het materiële recht werd al snel duidelijk dat een betrouwbaar watermerk enkel in staat is om bewijs te leveren voor het feit dat het op internet aangetroffen bestand bij de licentienemer hoort. Dat feit is vervolgens in de bewijsrechtelijke context nader onderzocht (par. 7.4). De effectiviteit van bewijsmiddelen wordt daar beoordeeld in het licht

[1] Als onderdeel van een gezamenlijk onderzoeksprogramma (IM-PACT) van het Vlaamse IBBT en het Nederlandse ICT-Regie op het gebied van digitale media is in samenwerking met IBBT-ICTRO (Vrije Universiteit Brussel) gezocht naar een technische oplossing voor het ontsluiten van digitale content via het toevoegen van verborgen informatie aan content door middel van watermerken. Zie par. 1.3.2 en par. 1.4.1.

van het te bewijzen feit waarvoor het middel wordt aangevoerd, en welke stellingen ten aanzien van dat feit en het bewijsmiddel zijn aangevoerd. Vanuit dat perspectief is vooral gekeken naar de vraag welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren over het te bewijzen feit waarvoor het watermerk wordt aangevoerd en op welke wijze de rechter deze stellingen moet beoordelen. Verweren ten aanzien van de toelaatbaarheid en betrouwbaarheid van het watermerk vormen de meest aannemelijke verweren om het watermerk direct haar effectiviteit te laten verliezen. Een ontoelaatbaar watermerk kan immers niet in de procedure worden toegelaten (par. 7.5) en ook een onbetrouwbaar watermerk zal door de rechter niet als bewijs worden geaccepteerd (par. 7.6). Dit hoofdstuk wordt afgesloten met een slotakkoord waarin kort wordt ingegaan op de vraag of het watermerk in het recht kan worden ingepast en welke waarde het watermerk in de praktijk kan hebben (par. 7.7).

7.2 Watermerken als technisch bewijsmiddel

Digitaal watermerken is kort gezegd een techniek om een boodschap te embedden in een digitaal signaal of gastobject. In dit onderzoek staat centraal het onwaarneembare digitale watermerk dat als doel heeft de licentienemer te kunnen achterhalen (traitor tracing). Bij het vaststellen van de gegevens van de licentienemer in het kader van traitor tracing komt het dan uiteindelijk neer op de vraag of het watermerk ten onrechte niemand kan vinden (vals negatief) en/of het watermerk mogelijk ten onrechte een onschuldige aanwijst (vals positief). Voor het bewijs is met name de laatste vraag van belang omdat in het eerste geval de rechthebbende er niet toe komt het watermerk als bewijsmiddel in te zetten. Voor de vraag of de rechthebbende het watermerk als product wil afnemen is de eerste vraag vanzelfsprekend wel van belang.

Het idee achter watermerken is dat iemand in de praktijk via een webwinkel bijvoorbeeld een film afneemt (licentienemer) door in te loggen en bepaalde gegevens in te voeren. Deze gegevens worden dan vervolgens door middel van een watermerk aan de film toegevoegd. Wanneer de film dan op internet wordt aangetroffen, kan het watermerk worden uitgelezen en de licentienemer worden aangesproken.

In de watermerkliteratuur is vooral aandacht voor het proces van watermerken dat bestaat uit het aanbrengen, verspreiden, detecteren en interpreteren van het watermerk. De aandacht richt zich dan voornamelijk op het hanteren van de juiste algoritmen en sleutels. Ook is er veel aandacht voor de aanvallen die mogelijk zijn op de onderdelen van dit proces en op maatregelen om deze aanvallen te weerstaan. Het resultaat van onderzoek naar watermerken levert dan een kansberekening op ten aanzien van de aanwezigheid van een bepaald watermerk en uiteindelijk een kansberekening dat het op internet aangetroffen bestand hoort bij een bepaalde licentienemer.

De primaire aandacht voor de techniek is vanuit de watermerkliteratuur logisch maar is voor het watermerk als bewijsmiddel slechts een deel van de puzzel. Dat komt voornamelijk omdat in de watermerkliteratuur de gegevens die in het watermerk worden gestopt als een vast gegeven worden beschouwd. In de praktijk bestaat het watermerk als bewijsmiddel dan uit twee elementen.

Ten eerste zal moeten worden aangetoond dat de gegevens die in het watermerk zijn aangebracht betrouwbaar zijn (authenticatie). Dat wil zeggen, dat de gedaagde of verdachte ook degene is die oorspronkelijk het werk (bestand) heeft aangeschaft (hierna: licentienemer). Bij een meerderheid van de afnemers zullen de juiste gegevens in de regel bekend zijn, bijvoorbeeld omdat een groot deel van de consumenten deze gegevens juist invoert of omdat zij al bekend zijn, bijvoorbeeld vanwege hun abonnement (bijv. pay-tv via KPN of Ziggo). Niet onbelangrijk is echter dat juist een groep afnemers die erop uit is om de bestanden te delen hun best zal doen de invoer van de gegevens te saboteren door bijvoorbeeld een valse naam op te geven of het bestand te verkrijgen door middel van iemand bij wie geen verhaal mogelijk is, zoals bij een verslaafde. Dit betekent ook dat de inzet van watermerken als bewijsmiddel zich er vooral op richt om eerlijke afnemers eerlijk te houden. Een belangrijke voorwaarde voor het slagen van het watermerk als bewijsmiddel is dat de licentienemer is wie hij zegt te zijn (authenticatie). Wanneer de rechthebbende of het Openbaar Ministerie (hierna: OM) erin slaagt te bewijzen dat de hier bedoelde gegevens juist zijn komt men ertoe te bewijzen dat het watermerk als techniek betrouwbaar is.

Ten tweede zal dan moeten worden bewezen dat het watermerk betrouwbaar is door aan te tonen dat het proces van aanbrengen tot interpreteren op een juiste wijze is verlopen. Daarbij zal duidelijk moeten worden dat de technieken die men gebruikt heeft in relatie tot het doel te verantwoorden zijn. Tevens zal de rechthebbende moeten aantonen dat de gekozen eigenschappen van het watermerk overeenkomen met het gewenste doel (traitor tracing). Daarnaast moet duidelijk worden gemaakt voor welk embed- en detectiemechanisme is gekozen. In bijna alle gevallen is er sprake van een bepaalde trade-off en zullen er keuzes moeten worden gemaakt. Om het watermerk als bewijsmiddel te kunnen gebruiken zal duidelijk moeten worden in hoeverre deze wisselwerking de betrouwbaarheid van het watermerk heeft beïnvloed. Tot slot zal ook aandacht moeten zijn voor de vraag in hoeverre de meest aannemelijke aanvallen van invloed zijn op de betrouwbaarheid van het watermerk als techniek. Daarvoor kan aansluiting worden gezocht bij de literatuur. Ook het ‘overleven’ van wedstrijden met als doel watermerken te kraken kan een indicatie zijn van de betrouwbaarheid van het watermerksysteem. Hierbij moet worden opgemerkt dat veel commerciële watermerken de gehanteerde systemen geheimhouden zodat in de literatuur en bij wedstrijden niet snel aanknopingspunten kunnen worden gevonden en de wederpartij zich al snel tot een deskundige zal moeten richten om zicht te krijgen op de betrouwbaarheid van het watermerk in kwestie.

Samengevat, wordt de betrouwbaarheid van watermerken als bewijsmiddel bepaald door twee elementen. Ten eerste door de invoer van juiste (persoons)gegevens. Ten tweede door het juist inzetten van de techniek van watermerken zelf. De betrouwbaarheid van het watermerk als

techniek is afhankelijk van de gewenste toepassing in relatie tot de inzet van de gebruikte eigenschappen, embed- en detectiemechanisme (algoritmen en sleutels) en de kans dat een aanval succesvol is uitgevoerd. Een betrouwbaar watermerk kan, aangenomen dat de gegevens die erin zijn opgenomen correct zijn, op grond van de literatuur dan ook enkel als bewijs dienen om aan te tonen dat het bestand aan de licentienemer toebehoort.

7.3 Watermerken en het vaststellen van auteursrechtinbreuk

De effectiviteit van het watermerk als juridisch bewijsmiddel wordt naast de technische mogelijkheden van het watermerk vooral bepaald door de rol die het watermerk krijgt in de context van het bewijsrecht. Het materiële recht bepaalt welke rol het watermerk kan spelen bij het vaststellen van auteursrechtinbreuk.

In zowel het Nederlandse als het Belgische civiele recht is er, overeenkomstig Europese richtlijnen, sprake van inbreuk op het auteursrecht wanneer een werk beschikbaar wordt gesteld voor het publiek en/of wordt gedistribueerd zonder dat degene die de handelingen verricht hiervoor toestemming heeft verkregen van de rechthebbende (licentie) of een beroep kan doen op de wettelijke beperkingen of uitzonderingen op de vermogensrechten van de auteur. Of er sprake is van een werk is zowel in Nederland als in België aan de rechter overgelaten en behoeft in beginsel geen bewijs. Het watermerk speelt voor het antwoord op die vraag dan ook geen rol. Dat geldt ook voor het feit dat het werk openbaar moet zijn gemaakt of verveelvoudigd. Dat het werk openbaar gemaakt of verveelvoudigd is, wordt in de regel duidelijk door te bewijzen dat het bestand op internet is aangetroffen. In de praktijk levert dat in deze gevallen weinig bewijsproblemen op. Beide hiervoor besproken handelingen leveren geen inbreuk op het auteursrecht op wanneer duidelijk wordt dat degene die het bestand op internet heeft geplaatst hiervoor toestemming had van de rechthebbende of een beroep kan doen op een wettelijke beperking, zoals de privékopie of het citaatrecht. De hier bedoelde uploader zal in de regel geen beroep kunnen doen op een van deze rechten. Wanneer de rechthebbende besluit het watermerk als bewijsmiddel in te zetten zal ook van toestemming voor het openbaar maken of verveelvoudigen van het werk geen sprake zijn. Het watermerk dient er als bewijsmiddel dan toe om een verband te leggen tussen de licentienemer en de inbreuk op het auteursrecht. Het watermerk is in geen geval voldoende om inbreuk op het auteursrecht als zodanig te bewijzen. Daarvoor zijn, zoals hiervoor besproken, meer vaststellingen nodig.

In zowel het Nederlandse als het Belgische strafrecht is voor de strafrechtelijke aansprakelijkheid vereist dat er met opzet inbreuk op het auteursrecht is gepleegd. Voor de invulling van het begrip ‘inbreuk op het auteursrecht’ wordt in beide landen aansluiting gezocht bij het civiele recht. In het strafrecht staat dan vooral de opzet centraal. Dat betekent dat de vermeende inbreukmaker zonder toestemming van de rechthebbende en zonder een beroep te kunnen doen op enige wettelijke beperking het werk openbaar heeft gemaakt dan wel verveelvoudigd heeft. Aangezien het watermerk geen meerwaarde kan leveren ten

aanzien van het strafrechtelijk opzetbegrip kan het watermerk als bewijsmiddel ook in het strafrecht enkel dienen om een verband te leggen tussen de licentienemer en de inbreuk op het auteursrecht.

Samenvattend kan worden gesteld dat het watermerk zowel naar Nederlands als Belgisch civiel en strafrecht geen mogelijkheden biedt om bewijs te leveren aan de invulling van het materiële recht. Als juridisch bewijsmiddel kan het dan ook enkel dienen om een verband te leggen tussen de licentienemer en de inbreuk op het auteursrecht. Het watermerk is in geen geval voldoende om inbreuk op het auteursrecht als zodanig te bewijzen. Daarvoor zijn, zoals hiervoor besproken, meer vaststellingen nodig.

7.4 Watermerken als effectief bewijsmiddel in de context van het bewijsrecht

De effectiviteit van het watermerk als bewijsmiddel wordt naast het materiële recht ook bepaald door de context van het bewijsrecht. De effectiviteit van bewijsmiddelen wordt naar Nederlands en Belgisch civiel recht beoordeeld in het licht van het te bewijzen feit waarvoor het middel wordt aangevoerd, en welke stellingen ten aanzien van dat feit en het bewijsmiddel zijn of kunnen worden aangevoerd. Vanuit dat perspectief moet vooral worden gekeken naar de vraag welke stellingen partijen redelijkerwijs kunnen en soms moeten aanvoeren ten aanzien van het te bewijzen feit waarvoor het watermerk als bewijs dient en op welke wijze de rechter deze stellingen moet beoordelen. Het feit dat de rechthebbende of het OM met een betrouwbaar watermerk wil bewijzen, is dat het bestand aan de gedaagde of verdachte toebehoort.

In zowel het Nederlandse als het Belgische civiele recht geldt ten aanzien van het geschil partijautonomie. Dat betekent dat het aan partijen is om stellingen aan te voeren en eventueel bewijs te leveren. In beide landen ligt de bewijslast van het hier centraal gestelde feit aan de zijde van de rechthebbende. Dat wil zeggen dat hij moet stellen en zo nodig moet bewijzen dat het bestand aan de licentienemer toebehoort. In beide landen zal de gedaagde voldoende verweer moeten voeren tegen deze stelling om te voorkomen dat de rechter het feit vaststelt. In tegenstelling tot België bestaat in Nederland na de fase van stellen en betwisten nog een mogelijkheid voor partijen om door middel van een bewijsaanbod en een verkregen bewijsopdracht aanvullend bewijs te leveren. De bewijsopdracht maakt voor partijen duidelijk waar volgens de rechter het bewijsprobleem zich bevindt. Het belangrijkste verschil is dan dat het partijen duidelijk wordt op welke punten de rechter kennelijk nog niet overtuigd is. In België is dat formeel minder duidelijk. Overigens moet aan dit verschil niet teveel waarde worden gehecht omdat de Nederlandse rechter veel zaken in de eerste fase al beslist en partijen om die reden al niet meer toekomen aan het vervullen van een eventuele opdracht die in de regel bestaat uit getuigenverhoor of een deskundigenbericht. Dit omdat partijen in beide landen al het (schriftelijke) bewijs zo snel mogelijk in de procedure moeten brengen.

Waar de rechthebbende het watermerk als bewijs aan zal voeren voor het te bewijzen feit dat het bestand aan de licentienemer toebehoort zal de gedaagde tegen deze stelling verweer willen voeren. De meest aannemelijke verweren liggen dan in het domein van de toelaatbaarheid (par. 7.5) en betrouwbaarheid van het watermerk (par. 7.6). Indien de rechter één van beide verweren succesvol acht dan is daarmee direct de effectiviteit van het watermerk aangetast. Een ander aannemelijk verweer is een verweer dat zich richt op een alternatieve verklaring voor het gestelde feit. Dit verweer raakt de effectiviteit van het watermerk in beginsel niet, omdat de gedaagde niet zozeer betwist dat het bestand bij hem hoort maar een alternatieve verklaring heeft voor dit feit. Zijn verweer bestaat er dan uit dat het bestand weliswaar zijn naam bevat maar dat het bestand door toedoen van een ander op internet is gekomen, bijvoorbeeld door een hack of virus. Hoewel dit een aantrekkelijk verweer is, zal het in de praktijk niet eenvoudig te voeren zijn. Ten eerste moet het gepresenteerde alternatief passen binnen de reeds vaststaande feiten en moet de rechthebbende het verweer niet eenvoudig kunnen weerleggen. Ten tweede zal de gedaagde zijn stelling, dat hij bijvoorbeeld is gehackt of een ander het bestand op internet heeft geplaatst, moeten onderbouwen. Het is voor de licentienemer in de praktijk lastig, maar niet onmogelijk om een succesvol verweer te voeren in termen van aansprakelijkheid ten aanzien van de inbreuk op het auteursrecht. Al was het maar omdat hij het ook daadwerkelijk niet kan hebben gedaan.

In de regel zal het echter niet eenvoudig zijn om verweer te voeren ten aanzien van het watermerk als bewijsmiddel. Dit is voornamelijk gelegen in het feit dat de gedaagde zijn stellingen zal moeten onderbouwen. Om aan die onderbouwing enig gewicht toe te kennen zal hij zich moeten laten voorlichten door een deskundige, omdat hij in de regel bij commerciële watermerken weinig aanknopingspunten zal vinden in de beschikbare literatuur. Het inschakelen van een deskundige stelt de gedaagde voor de keuze of hij kosten wil maken voor een deskundige. Naast de kosten speelt daarbij ook een rol dat vooraf niet duidelijk is of de resultaten van het deskundigenverslag in het voordeel van de gedaagde zullen werken of niet. De kosten van een IE-procedure waarin een volledige proceskostenveroordeling mogelijk is en het vooruitzicht dat hij kosten moet maken om een deskundige in te schakelen om de effectiviteit van het watermerken te onderzoeken, maakt het watermerk voor de rechthebbende een aantrekkelijk handhavingsmiddel. De inzet ervan zal er namelijk toe bijdragen dat de gedaagde eerder bereid is te schikken. Een schikking is voor alle partijen de goedkoopste oplossing en voorkomt een gang naar de rechter. Dat heeft voor de rechthebbende vooral als voordeel dat het watermerk ook in termen van preventie dienst kan doen en ook de toelaatbaarheid en betrouwbaarheid van het watermerk als bewijsmiddel niet snel zal worden getest. Dat heeft tot gevolg dat het watermerk als handhavingsmiddel effectief kan zijn zonder ooit op zijn betrouwbaarheid te zijn getoetst. In het civiele recht bestaat weliswaar de mogelijkheid dat de rechter zelf een deskundige benoemt of deze benoemt op verzoek van partijen, maar in de regel is daar niet snel aanleiding toe. Het is immers aan partijen om stellingen aan te voeren. Wanneer de rechthebbende het watermerk in de vorm van een rapportage aanvoert ter onderbouwing van zijn stelling en de wederpartij

eventueel verweer voert, is de rechter in de regel snel van oordeel dat hij voldoende gronden vindt om het geschil te beslissen. Dat maakt het watermerk los van de bewijswaarde tot een strategisch middel voor de handhaving van het auteursrecht.

In een strafrechtelijke context werkt het watermerk als bewijsmiddel niet heel veel anders. De bewijslast in het strafrecht ligt geheel bij het OM, wat in theorie betekent dat de verdachte achterover kan leunen. In de praktijk zal hij echter verweer moeten voeren om te voorkomen dat de rechter enkel zijn oordeel vormt op het bewijs dat het OM aanlevert. In theorie heeft de rechter zelf ook de mogelijkheid om de zaak te onderzoeken. Dat zal hij in de praktijk echter vooral doen wanneer hij het vermoeden heeft dat het watermerk echt ontoelaatbaar of onbetrouwbaar is. In die zin doet de verdachte er goed aan verweer te voeren. Verweren die zien op de toegang tot deze bestanden door hackers hebben zonder duidelijke aanwijzingen, ook in het strafrecht, geen succes.

Samengevat zal de gedaagde of verdachte in de praktijk voldoende verweer moeten voeren om te voorkomen dat de rechter het door de rechthebbende of OM aangevoerde feit, dat het op internet aangetroffen bestand aan de licentienemer toebehoort, vaststelt. Om verweer te kunnen voeren ten aanzien van het watermerk zal in de regel een deskundige nodig zijn die de gedaagde of verdachte voor de vraag stelt of de daarmee gepaard gaande kosten opwegen tegen het voeren van een rechtszaak. Het watermerk vormt daarmee in ieder geval een strategisch middel om het niet tot een rechtszaak te laten komen en een schikking te accepteren.

7.5 Watermerken als toelaatbaar bewijsmiddel

Alleen watermerken die de rechter toelaatbaar acht kunnen voor het bewijs worden gebruikt. Daarvoor moet het watermerk gekwalificeerd kunnen worden als een wettig bewijsmiddel en mag de verkrijging van het bewijs geen dusdanige inbreuk maken dat de rechter daaraan het gevolg verbindt dat het bewijs moet worden uitgesloten.

In zowel Nederland als België zal de kwalificatie van het watermerk als bewijsmiddel geen problemen opleveren. In Nederland geldt een zogenoemd systeem van vrij bewijs waardoor in beginsel alles tot het bewijs is toegelaten. België kent in tegenstelling tot het Nederlandse civiele recht een gesloten systeem van bewijs. Ten aanzien van het strafrecht is de situatie omgekeerd en kent Nederland een gesloten systeem van bewijs en kent België een open systeem. In de praktijk wordt in beide landen het gesloten stelsel ruim geïnterpreteerd waardoor technische middelen vrijwel altijd als juridisch bewijsmiddel kunnen worden gekwalificeerd. Daarnaast zal het watermerk in de regel als schriftelijk bewijs worden ingediend in de vorm van een rapportage of verslag. Schriftelijk bewijs is in beide landen en beide rechtssystemen altijd mogelijk. Er is om die reden zowel in Nederland als in België weinig reden om aan te nemen dat het watermerk in zowel een civiele als in een strafprocedure niet als juridisch bewijsmiddel kan worden gekwalificeerd. Daarnaast is

gekeken naar de vraag of het watermerk als bewijsmiddel op een andere wijze ontoelaatbaar zou zijn. Daarbij is vooral gekeken naar de vraag of het watermerk is verkregen in strijd met privacyrechten van de licentienemer.

Watermerken kunnen door de rechter ook worden uitgesloten als juridisch bewijsmiddel wanneer het watermerk is verkregen door inbreuk op een (grond)recht van de licentienemer. In het kader van de grondrechtendiscussie heeft het Hof van Justitie EU bij het inzetten van technologie voor de handhaving van het auteursrecht duidelijk gemaakt dat het permanent filteren van het internet op de inhoud van de bestanden in strijd is met ten minste drie grondrechten: de vrijheid van ondernemerschap, het recht op bescherming van persoons-gegevens en de vrijheid om informatie te ontvangen of te verstrekken. Het Hof heeft zich hiermee enkel uitgesproken over de grenzen van een algemeen filtersysteem. Het Hof acht bij filtering van netwerken een inbreuk op het privacyrecht mogelijk, wanneer er sprake is van een systematische analyse van alle inhoud die het gebruik van het systeem veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Daarvan is hier geen sprake. Anders dan bij het hier voorgestelde systeem vindt bij watermerken geen systematische analyse plaats van alle inhoud. Behoudens een mogelijke inbreuk op privacyrechten van de licentienemer lijkt het watermerk de toets van het Hof te kunnen doorstaan. In tegenstelling tot het in deze zaak centraal gestelde filtersysteem wordt bij watermerken van een derde noch een (algemene) toezichtsrol verwacht, noch komen de kosten voor de invoering voor zijn rekening. Er is in die zin geen reden om aan te nemen dat iemand in zijn vrijheid van ondernemerschap wordt aangetast. Ook is er weinig reden om aan te nemen dat de vrijheid om informatie te ontvangen of te verstrekken bij watermerken wordt aangetast nu het mogelijk is om in het kader van de vrijheid van informatie voldoende onderscheid te maken tussen legale en illegale inhoud. Bovendien koppelt het Hof dit onderscheid aan de toepassing die ertoe zou kunnen leiden dat communicatie met legale inhoud wordt geblokkeerd. In tegenstelling tot het voorgestelde filtersysteem is er bij watermerken geen sprake van blokkering van de inhoud waardoor de ernst van de sanctie in relatie tot de mate van onderscheid in een ander perspectief komt te staan. Ook maakt het watermerksysteem bij het zoeken naar auteursrechtelijk beschermde werken op internet alleen gebruik van zogenoemde openbare bronnen waardoor een verdere aantasting van grondrechten zoals privacy veelal beperkt zal zijn.

Om na te gaan of en zo ja onder welke omstandigheden de rechthebbende bij het verwerken van gegevens in strijd handelt met de privacy van de licentienemer is gekeken naar de nationale privacywetten van Nederland en België.

Zowel de Nederlandse Wet bescherming persoonsgegevens (Wbp) als de Belgische Wet met betrekking tot de verwerking van persoonsgegevens (WVP) komen voor een belangrijk deel voort uit de Europese privacyrichtlijn en hebben om die reden vergelijkbare bepalingen ten aanzien van de voorwaarde waaronder de gegevens in het watermerk mogen worden verwerkt. Schending van de in deze wetten opgenomen zorgvuldigheidsnormen vormen dan

ook een onrechtmatige daad. In het bijzonder moet hierbij worden gedacht aan de wijze waarop de persoonsgegevens worden verkregen, verwerkt en bewaard. Voor watermerken is het van belang dat iedere verwerking gebaseerd moet zijn op een zogenoemde verwerkingsgrondslag. De ondubbelzinnige toestemming van de licentienemer is in beide landen de meest voor de hand liggende grondslag voor de verwerking van persoonsgegevens. De rechthebbende zal in andere gevallen de licentienemer tenminste moeten informeren over de verwerking van de persoonsgegevens als over het doel ervan, inclusief eventuele doorgifte van zijn gegevens. Het recht op privacy is in beide landen geen absoluut, maar een functioneel recht waarbij in het kader van de rechtmatigheid een balans moet worden gezocht tussen verschillende rechten van partijen. Wanneer de rechter tot de conclusie komt dat er sprake is van inbreuk op het privacyrecht van de licentienemer komt de rechter toe aan de vraag of de schending gerechtvaardigd was. Bij watermerken zal de rechter dan een afweging moeten maken tussen enerzijds het belang van de licentienemer bij eerbiediging van zijn persoonlijke levenssfeer en anderzijds het belang van de rechthebbende bij het beschermen van zijn intellectuele eigendom. Bij de beoordeling van de ernst van de inbreuk kan ook de aard en de mate van intimiteit van de informatie van groot gewicht zijn. De ernst van de inbreuk zal bij watermerken, mede vanwege de aard en zeer beperkte mate van intimiteit, gering worden geacht. Een inbreuk op de nationale privacywetten zal tot de conclusie leiden dat het bewijs in strijd met de wet, en dus onrechtmatig is verkregen.

De volgende vraag die dan beantwoord dient te worden is of aan een onrechtmatig verkregen watermerk het gevolg moet worden verbonden dat dit bewijsmiddel van het bewijs moet worden uitgesloten. Daar lijkt weinig reden toe. Naar Nederlands civiel recht heeft de Hoge Raad recent in het arrest Achmea/Rijnberg er expliciet voor gekozen dat in civiele zaken het algemene maatschappelijke belang dat de waarheid in rechte aan het licht komt in beginsel zwaarder weegt dan het belang van uitsluiting van bewijs. Het uitsluiten van het bewijs is volgens de Hoge Raad dan ook slechts gerechtvaardigd, indien sprake is van bijkomende omstandigheden. In België kiest het Hof van Cassatie er sinds 2008 ook in civiele zaken voor om het gebruik van onrechtmatig bewijs enkel van het bewijs uit te sluiten wanneer (1) de overtreden norm of formaliteit op straffe van nietigheid is voorgeschreven; (2) de onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast en (3) het recht op een eerlijk proces is geschaad (Antigoon-leer). Anders dan de Nederlandse Hoge Raad heeft het Hof van Cassatie in België niet expliciet duidelijk gemaakt dat de waarheidsvinding in beginsel zwaarder weegt dan het belang van uitsluiting van bewijs. Evenals de Hoge Raad heeft ook het Hof van Cassatie echter een behoorlijke drempel opgeworpen om onrechtmatig verkregen bewijs van het bewijs uit te sluiten.

Wanneer het OM zou besluiten de vermeende licentienemer te vervolgen dan komt ten aanzien van het watermerk in beide landen de vraag naar voren of het OM bewijs mag gebruiken dat door de rechthebbende op een onrechtmatige wijze is verkregen. Zolang de overheid geen bemoeienis heeft gehad met de onrechtmatige verkrijging van het bewijs, is er in de regel zowel naar Nederlands als Belgisch strafrecht geen reden om aan te nemen dat

onrechtmatig verkregen bewijs van het bewijs zal worden uitgesloten. Bij watermerken zal de overheid in de regel geen bemoeienis hebben met het aanbrengen van watermerken in content van private partijen.

Schending van het recht op privacy werd ook voor de hiervoor genoemde arresten in het Nederlandse en Belgische civiele recht en strafrecht zelden gesanctioneerd met uitsluiting van het bewijs. Het valt echter ook op dat er in de civiele rechtspraak zelden andere consequenties worden verbonden aan het schenden van de privacy. Het uitsluiten van bewijs mag, mede in het licht van de waarheidsvinding, een onwenselijke sanctie zijn, maar het geheel ontbreken van sancties doet ook geen recht aan de situatie en aan het juridisch systeem. Zoals de licentienemer zich in het kader van de waarheidsvinding niet mag verschuilen achter zijn recht op privacy, zo zou ook de rechthebbende geen louter voordeel moeten kunnen halen uit zijn onrechtmatig handelen. De rechter zou naar mijn mening bij een schending van het recht op privacy dan ook meer aandacht moeten hebben voor de sanctionering daarvan. Bijvoorbeeld door andere sancties te verbinden aan het schenden van privacyregels, zoals het matigen van de toe te kennen schadevergoeding, het weigeren van een vordering tot afgifte bij een ISP of het toekennen van een schadevergoeding vanwege het schenden van de privacy. Dit temeer omdat de rechthebbende zelf de controle heeft over de wijze waarop hij de gegevens van de licentienemer verkrijgt en daarmee omgaat. Aangenomen mag worden dat hij dit zorgvuldig doet omdat er inmiddels voldoende kennis en middelen zijn om dit ook in een online omgeving zorgvuldig uit te voeren.

Voor een zorgvuldige uitvoering van deze privacyregels kan de rechthebbende aansluiting zoeken bij de in 2008 door de Amerikaanse burgerrechtbeweging Center for Democracy & Technology (CDT) gepubliceerde ‘Privacy Principles for Digital Watermarking’ waarmee zij een concreet toetsingskader heeft ontwikkeld dat voldoet aan Europese privacyrichtlijnen en de implementatie daarvan in de Nederlandse en Belgische wetgeving. Deze beginselen vragen aandacht voor (1) Privacy by design, waarmee wordt bedoeld dat er vanaf het begin van de ontwikkeling aandacht moet zijn voor privacy; (2) het vermijden van direct bruikbare informatie, zodat zelfs wanneer de informatie openbaar wordt deze niet direct bruikbaar is; (3) het informeren van de gebruiker; (4) het beperken van de toegang tot het uitlezen van watermerken; (5) het adequaat reageren als de watermerkalgoritmen zijn gekraakt; (6) de bescherming van de databanken; (7) het beperken van het gebruik voor andere doeleinden en tot slot (8) de zorg voor toegang en wijzigingsmogelijkheden voor gebruikers.

Samengevat is er geen reden om aan te nemen dat het watermerk niet als bewijs toelaatbaar is. Het watermerk kan in beide landen en rechtsgebieden zonder problemen als wettig bewijsmiddel worden gekwalificeerd. Hoewel het niet is uitgesloten dat het watermerk in strijd met privacyregels is verkregen zal het watermerk in de regel, mede in het licht van de waarheidsvinding, niet van het bewijs worden uitgesloten. Een verweer dat gericht is op het uitsluiten van het watermerk voor het bewijs zal zowel naar Nederlands als Belgisch civiel- en strafrecht dan ook weinig kans van slagen hebben.

7.6 Watermerken als betrouwbaar bewijsmiddel

Tot slot rest de vraag wanneer het watermerk door de rechter als een betrouwbaar bewijsmiddel kan worden aanvaard.

Het watermerk wordt zowel in een civiele als in een strafrechtelijke procedure in de regel gepresenteerd in de vorm van schriftelijk bewijs. Om te beoordelen of het watermerk een betrouwbaar bewijsmiddel is, is onderzocht wanneer de rechter aan de rapportage van de rechthebbende voldoende bewijskracht kan toekennen om het watermerk als bewijsmiddel te accepteren om daarmee het feit dat het bestand aan de licentienemer toebehoort vast te stellen.

Ten eerste moet de rapportage voldoen aan de algemene eisen die gesteld worden aan (digitaal) forensisch onderzoek. Dat betekent dat aandacht moet zijn voor de juiste vraagstelling, methodiek, en de wijze waarop het onderzoek tot stand is gebracht. Dat betekent dat de organisatie in staat moet zijn het gehele proces inzichtelijk te maken en te laten controleren. In het verslag zal met andere woorden duidelijk gemaakt moeten worden op welke wijze de kwaliteit van het onderzoek is gewaarborgd. De rechthebbende moet in staat zijn om door middel van een chain of custody, een chain of evidence te maken. Bijvoorbeeld om aan te kunnen tonen dat de koppeling van de gegevens van de licentienemer en het watermerk juist is of dat het op internet aangetroffen bestand ook daadwerkelijk het bestand is waarop onderzoek is verricht en waarin het desbetreffende watermerk is gevonden. Dit proces is niet nieuw maar dient wel aandacht te krijgen bij de beoordeling van het watermerk als bewijs en bij het opstellen van het verslag.

Ten tweede moet uit het verslag duidelijk worden of het watermerk een betrouwbaar bewijsmiddel is. De betrouwbaarheid van het watermerk ziet in beginsel op twee aspecten. De gegevens die in het watermerk worden gestopt moeten juist zijn (authenticatie licentienemer) en het watermerken als techniek moet betrouwbaar zijn. Dat wil zeggen dat dezelfde gegevens die in het watermerk zijn gestopt er ook weer uit te halen zijn. Dat betekent ook dat er in de rapportage niet alleen aandacht moet zijn voor de techniek van het watermerken, maar ook voor de wijze waarop de authenticatieprocedure is ingericht en waarom deze procedure in dit geval betrouwbaar is. Daarbij dient tevens aandacht te zijn voor de meest aannemelijke verweren die de gedaagde kan voeren ten aanzien van de betrouwbaarheid van het watermerk als bewijsmiddel. Bij deze verweren staat de vraag centraal onder welke omstandigheden watermerken de verkeerde uitkomst kunnen geven. In de rapportage zal om die reden aandacht moeten zijn voor de vraag hoe groot de kans is dat er fouten zijn gemaakt in het authenticatieproces (verkeerde naam), fouten bij het inzetten van de techniek van watermerken waardoor er sprake kan zijn van een fout-positief, en de kans dat iemand anders het bestand met ‘zijn’ traitor tracingscode en zonder zijn medeweten heeft verspreid (vals watermerk). En in welke verhouding deze kans moet worden begrepen. In de rapportage zal onder meer duidelijk moeten worden welke maatregelen zijn genomen om voornoemde situaties te voorkomen. Om het watermerk als techniek betrouwbaar te achten zal in de

rapportage aandacht moeten zijn voor het doel en het gastobject waarin het watermerk is geplaatst. Deze gegevens moeten duidelijk maken of de gekozen watermerktechniek geschikt is voor het object dat het moet beschermen. Tevens zal aandacht moeten zijn voor de watermerktechniek zelf. Dat betekent dat duidelijk zal moeten worden of de gebruikte sleutels en algoritmen betrouwbaar zijn. Hierbij zal ook duidelijk moeten worden op welke wijze de watermerken worden aangebracht en worden gedetecteerd. Vervolgens moet in de rapportage duidelijk worden wat de meest aannemelijke aanvallen zijn op de gekozen watermerken. En of en zo ja welk effect dat heeft op de betrouwbaarheid van het watermerk als bewijsmiddel in de zaak waarin de rapportage wordt ingebracht.

Ten derde is het van belang dat de rechter de resultaten van het rapport op de juiste waarde weet te schatten. Dat betekent dat de rechter aandacht moet hebben voor de valkuilen die er bestaan bij het komen tot een bewijsbeslissing, in het bijzonder ten aanzien van de invloed die getallen hebben op lezers van het rapport. De rechter zal zich rekenschap moeten geven dat het lezen van een rapportage niet eenvoudig is. Evenals bij rapportages ten aanzien van DNA-bewijs zal ook bij watermerken in het verslag gebruik worden gemaakt van verschillende kansberekeningen. Onderzoek naar DNA-bewijs wijst uit dat juristen moeite hebben met het lezen van deze verslagen. Zelfs juristen die aangaven de rapporten te begrijpen bleken vaak niet in staat om de conclusie van het rapport op een juiste wijze te beschrijven. Dit gegeven zou de rechter waakzaam moeten maken dat op zichzelf betrouwbare informatie ook tot een juiste bewijsbeslissing leidt. Een onjuiste interpretatie van de gerapporteerde onderzoeks-resultaten kan immers leiden tot misvattingen over de sterkte van watermerken als bewijs. Vanuit het perspectief van de rechthebbende duiden deze onderzoeken op een risico bij het inzetten van watermerken als bewijs. Tegen deze achtergrond kunnen zelfs betrouwbare watermerken het watermerk nog ineffectief maken.

De kennis en ervaring die in de forensische literatuur is beschreven in het Nederlandse strafrecht is veelal opgedaan naar aanleiding van verschillende rechterlijke dwalingen en die voor het Nederlandse civiel recht zijn vertaald door De Bock in haar bewijswaarderings-maatstaf moeten bijdragen aan de gevraagde waakzaamheid bij het vaststellen van feiten. Dit geldt ook en mogelijk zelfs ‘zeker’ bij digitaal forensisch bewijs.[2] Vooral in zaken waarin er geen andere sporen zijn dan digitale sporen en digitaal bewijs derhalve het enige bewijs is, is oplettendheid vereist. Anders dan in een zaak waarin DNA als bewijs wordt gebruikt is de bron bij digitaal bewijs fragiel en zijn digitale sporen vaak de enige sporen. Dit terwijl digitale sporen perfect nagemaakt kunnen worden en tegenbewijs, mede vanwege de kosten, lastig te leveren kan zijn.

[2] Zie voor de maatstaf van De Bock, par. 4.2.3.1. ‘Een feit is voor de civiele rechter bewezen wanneer uit de beschikbare bewijsmiddelen redelijkerwijs kan worden afgeleid dat het feit zich heeft voorgedaan, en uit die bewijsmiddelen niet even goed kan worden afgeleid dat hetgeen de wederpartij met betrekking tot dat feit stelt, zich heeft voorgedaan, terwijl zich evenmin de situatie voordoet dat bewijsmateriaal dat redelijkerwijs verwacht mocht worden ontbreekt.’

Samengevat zal de rechter bij het beoordelen van de bewijskracht moeten beoordelen of het verslag voldoet aan de algemene eisen die aan forensische onderzoeksverslagen worden gesteld. Daarnaast zal de rechter moeten beoordelen of voldoende ingegaan is op de betrouwbaarheid van zowel watermerken als techniek als op de betrouwbaarheid van de (persoons)gegevens die het watermerk als boodschap draagt.

7.7 Slotakkoord

Aan het einde van dit onderzoek is het tijd om de balans op te maken. Met behulp van de centrale vraagstelling of een niet-waarneembaar digitaal watermerk dat als doel heeft de licentienemer te traceren, in Nederland een effectief juridisch bewijsmiddel vormt bij de handhaving van inbreuk op auteursrecht op digitaal beschikbaar gestelde foto's, muziek en video op internet worden hierna twee onderwerpen behandeld. Eerst zal antwoord worden gegeven op de vraag of het watermerk in het Nederlandse rechtssysteem kan worden ingepast (par. 7.7.1). Daarna wordt kort antwoord gegeven op de centrale vraagstelling, of het watermerk een effectief bewijsmiddel kan vormen in het Nederlandse recht en zo ja onder welke voorwaarden (par. 7.7.2). Tot slot zal kort de waarde van watermerken als auteursrechtelijk handhavingsmiddel worden besproken (par. 7.7.3).

7.7.1 Inpassingstoets: technische output voor juridische input

Bij de inzet van nieuwe technologie is het steeds de vraag of en op welke wijze deze in het recht kan worden ingepast. Voor watermerken is in dit onderzoek de vraag gesteld of het een effectief bewijsmiddel kan zijn bij de handhaving van het auteursrecht. De vraag of het watermerk dan in het rechtssysteem een plaatsvindt, is voor de beantwoording van de centrale vraagstelling een vraag die daaraan voorafgaat. Het watermerk kan immers slechts een effectief bewijsmiddel vormen wanneer het als bewijsmiddel kan worden toegelaten en in die zin in het systeem van het recht past.

Zoals uit hoofdstuk 4 en 5 blijkt is er geen reden om aan te nemen dat het watermerk niet als bewijsmiddel zou kunnen worden toegelaten. Het watermerk is tegelijk ook niet van dien aard dat er vragen rijzen of het mogelijk een onwenselijke techniek is. Ethische vragen, zoals deze werden gesteld bij de introductie van DNA als bewijs spelen geen rol bij de in dit onderzoek centraal gestelde watermerken. De wenselijkheid van een dergelijk bewijsmiddel is dan verder aan de samenleving overgelaten. Het watermerk kan als bewijsmiddel in die zin een plaats vinden in zowel het Nederlandse als Belgische civiele en strafrecht.

De volgende vraag die gesteld zou kunnen worden is of de wetgever het watermerk als bewijsmiddel van een zodanige status moet voorzien dat het, bijvoorbeeld overeenkomstig de elektronische handtekening, een eigen plaats in het recht krijgt. Die vraag zou ik negatief beantwoorden. Ten eerste lijkt het mij in het licht van het niet onnodig produceren van regels aan te bevelen dat de wetgever terughoudend is bij het formuleren van nieuwe wetgeving. Het

lijkt mij om die reden dan ook als eerste een kwestie van afwachten hoe dit middel zich in de praktijk ontwikkelt (technisch en juridisch) en dan de vraag beantwoorden of er behoefte bestaat aan een eigen plaats in het recht, bijvoorbeeld door het invoeren van een (bewijs)vermoeden. Ten tweede zal erop voorhand weinig maatschappelijk draagvlak zijn voor het instellen van een dergelijk bewijsvermoeden. Temeer omdat aan de handhaving van het auteursrecht minder maatschappelijk belang lijkt te worden gehecht dan aan de veiligheid van en het vertrouwen in elektronische communicatie, zoals bij de elektronische handtekening. Dit laatste argument is overigens wel afhankelijk van de toepassing van watermerken. Ten aanzien van watermerken met een authenticatiedoel ten behoeve van bijvoorbeeld paspoorten of rijbewijzen is een Europese richtlijn vergelijkbaar met die van de elektronische handtekening niet ondenkbaar. De wenselijkheid daarvan is overigens weer een vraag die dan opnieuw gesteld moet worden.

7.7.2 Randvoorwaarden: juridische input voor technische output

Voor de effectiviteit van het watermerk als bewijsmiddel zal bij de verdere ontwikkeling (en inzet) van watermerken rekening moeten worden gehouden met de privacy van gebruikers en de vrijheid van informatie. Verder is het voor het gebruik van het watermerk als bewijsmiddel verder van belang dat bij het verzamelen en analyseren van het watermerk wordt gehandeld in overeenstemming met de geldende forensische principes. Voor de beoordeling van het watermerk als juridisch bewijsmiddel is meer wetenschappelijk bewijs van de betrouwbaarheid van het watermerk gewenst, bijvoorbeeld door het ontwikkelen van (wetenschappelijke) standaarden. Deze onderdelen zullen hieronder nog kort worden toegelicht.

Houd rekening met privacy en de vrijheid van informatie

Eerder is geconstateerd dat in het kader van toelaatbaar bewijs zowel in Nederland als in België enkel bij grove schendingen van privacy leiden tot uitsluiting van het bewijs. Hiervan zal bij watermerken niet snel sprake zijn. Ook worden er in de jurisprudentie nauwelijks andere sancties verbonden aan een schending van deze rechten. Daaruit mag niet de conclusie worden getrokken dat de inrichting van een systeem geen juridische consequenties kan hebben. Een overtreding van privacyregelgeving blijft desondanks een onrechtmatige handeling waarvoor de gedaagde dan wel de nationale toezichthouder de verantwoordelijke op kan aanspreken. Daarnaast moet erop worden gewezen dat wanneer erop geen enkele wijze rekening wordt gehouden met de privacy van de licentienemer een rechter sneller geneigd zal zijn de situatie als een ernstige schending van de privacyrechten te beoordelen, waarvoor uitsluiting wel in de rede ligt. Vervolgens kan er nog op worden gewezen dat de rechter wel andere sancties dan bewijsuitsluiting kan verbinden aan het schenden van privacyregels, zoals het matigen van de toe te kennen schadevergoeding of het verlagen van de strafrechtelijke sanctie.

Het voorgaande maakt duidelijk dat het watermerk als bewijsmiddel op grond van een schending van privacyregels weliswaar niet snel tot uitsluiting van het bewijs leidt maar dat het veronachtzamen van privacy direct dan wel in de toekomst consequenties kan hebben voor het business model wat het verstrekken van licenties voor watermerksoftware uiteindelijk ook is. Het is om die reden verstandig om rekening te houden met privacy van de licentienemer. Dit kan door persoonsgegevens niet identificeerbaar te maken voor de rechthebbende (Chinese Walls) door deze bijvoorbeeld onder te brengen bij een TTP en een transparante procedure op te stellen waarin wordt vastgelegd onder welke voorwaarden de rechthebbende/exploitant van de content toegang krijgt. Andere technische oplossingen zijn mogelijk zolang de persoonsgegevens maar voldoende beschermd worden.

In het kader van het voorlichten van de gebruiker over de aanwezigheid van het watermerk kan hij er tevens op worden gewezen dat hijzelf medeverantwoordelijk is voor het bewaken van zijn privacy. Bijvoorbeeld door er expliciet op te wijzen dat hij het in de eerste plaats zelf in de hand heeft dat werken die ‘zijn watermerk’ bevatten niet verspreid raken.

Het Hof van Justitie EU maakt in de Sabam-zaak duidelijk dat het in het kader van de vrijheid van informatie het bij een filtersysteem onwenselijk is dat er onvoldoende onderscheid gemaakt wordt tussen legale en illegale inhoud. Dat betekent voor watermerken dat het wenselijk is dat er bij het inrichten van het watermerkproces aandacht is voor het maken van dit onderscheid. In de praktijk kan daarbij worden gedacht aan de mogelijkheid om tussen de opsporing van een werk en de detectie van het watermerk een stap in te bouwen waarbij nogmaals wordt gekeken naar de vraag of er inbreuk wordt gemaakt op het werk door ook rekening te houden met wettelijke uitzonderingen die gelden in het auteursrecht. Om verdere zoekkosten te beperken is het wel raadzaam om in het watermerk op te nemen of de licentienemer beschikt over een licentie die bijvoorbeeld verdere distributie op het internet toestaat. In dat geval zal in veel gevallen direct duidelijk zijn of er sprake is van een schending van de licentie-overeenkomst of niet.

Handel volgens forensische principes

Door watermerken als juridisch bewijs te gebruiken zal de rechthebbende er rekening mee moeten houden dat hij of zijn dienstverlener vanaf het begin handelt in overeenstemming met de geldende eisen van digitaal forensisch onderzoek. Een dergelijke organisatie draagt niet alleen bij aan de betrouwbaarheid van het watermerk als bewijsmiddel maar maakt het ook mogelijk later partijen en de rechter te informeren over bijvoorbeeld de gevoerde chain of custody.

Ontwikkel (wetenschappelijke) standaarden

Naast de belangrijke bruggen die geslagen kunnen worden tussen juristen en experts zou het vanuit het juridische perspectief een aanbeveling zijn om in het kader van de betrouwbaarheid

en beoordeling van systemen tijd te investeren in het ontwikkelen van standaarden en beoordelingsprotocollen. Deze standaarden lijken in de praktijk nauwelijks te bestaan en ook niet van de grond te komen. Toch wordt er ook in de watermerkliteratuur van tijd tot tijd aandacht gevraagd voor het ontwikkelen van standaarden. Hoewel standaarden niet de oplossing zijn en het niet hebben van standaarden niet alles zegt over de betrouwbaarheid van een watermerksysteem, zou het een impuls geven aan de rechtspraktijk. Het geeft juristen voor en tijdens een juridische procedure een beter beoordelingskader. Dat die rechtspraktijk ook voor de watermerkwetenschappers van belang is mag blijken uit de vele inleidingen van de verschillende bèta-wetenschappelijke artikelen die in veel gevallen de legitimatie van het onderzoek vinden in de handhaving van het auteursrecht. Watermerken zouden aan effectiviteit winnen wanneer er meer wetenschappelijke standaarden zouden komen.

7.7.3 Valorisatie: waarde van watermerken als bewijsmiddel

Op de centrale vraagstelling of het watermerk een effectief bewijsmiddel is, is in de voorgaande paragrafen uitvoerig ingegaan. De twee belangrijkste elementen die de bewijswaarde van een watermerk kunnen aantasten zijn de toelaatbaarheid en betrouwbaarheid van het watermerk. In hoofdstuk 5 en 6 is uitgebreid aandacht besteed aan de voorwaarde waaronder het watermerk toelaatbaar en betrouwbaar kan worden geacht. De belangrijkste conclusie daaruit is dat het watermerk een effectief bewijsmiddel kan zijn en dat de rechthebbende de bewijswaarde van het watermerk voor een belangrijk deel zelf in de hand heeft door zorgvuldig om te gaan met de (persoons)gegevens van de licentienemer en door een goede betrouwbare rapportage op te stellen wanneer hij het watermerk als bewijsmiddel wil gaan gebruiken. Juridisch gezien zijn weinig obstakels ter verwachten wanneer (technisch) duidelijk kan worden gemaakt dat het watermerk een betrouwbaar bewijsmiddel is. Vooralsnog lijkt de uitdaging bij de inzet van watermerken dan ook meer van technische dan van juridische aard.

Uit het voorgaande onderzoek is duidelijk geworden dat een betrouwbaar watermerk als effectief bewijsmiddel kan dienen om een verband te leggen tussen het op internet aangetroffen bestand en de licentienemer. Met het beantwoorden van de vraagstelling komt het verslag ten aanzien van het onderzoek teneinde. De laatste jaren is er in toenemende mate aandacht voor kennisvalorisatie dat in navolging van de Landelijke Commissie Valorisatie kan worden omschreven als ‘het proces van waardecreatie uit kennis, door kennis geschikt en/of beschikbaar te maken voor economische en/of maatschappelijke benutting en te vertalen in concurrerende producten, diensten, processen en nieuwe bedrijvigheid’.[3] Om die reden zal ik kort buiten het domein van de vraagstelling treden door mijn gedachten te laten gaan over de vraag wat volgens mij de waarde van het watermerk als auteursrechtelijk handhavingsmiddel is of kan zijn.

[3] Zie o.m. het rapport Waardevol - Indicatoren voor Valorisatie van het Rathenau Instituut (Drooge e.a. 2011).

De waarde van het watermerk als bewijsmiddel is afhankelijk van het doel dat de rechthebbende voor ogen heeft. Er is brede consensus dat de oplossing voor het auteursrechtelijke handhavingsprobleem schuilt in een mix van oplossingen (regulering), waarvan een oplossing met behulp van techniek er één is.[4] In het licht van het tegengaan van het verspreiden van auteursrechtelijk beschermde content kan het watermerk worden ingezet ten aanzien van twee belangrijke groepen (par. 3.2.2). Ten eerste kan het watermerk worden gebruikt om de groep consumenten die wel een licentie afsluiten 'eerlijk te houden', door met behulp van watermerken drempels op te werken om tot verspreiding van de werken over te gaan. Watermerken sluit voor die groep goed aan bij hun drijfveren (o.m. angst voor sancties) om kort gezegd niets illegaals te doen. Ten tweede kan watermerken worden ingezet om de verspreiding door de 'scene', een kleine groep die technisch vaardig is en uit is op de verspreiding van de werken, te vertragen. De winst voor de rechthebbende is dan om bijvoorbeeld films zo lang mogelijk van het internet te houden en daarmee aan bioscopen en pay-tvkanalen de mogelijkheid te bieden unieke content aan te bieden.

Watermerken als bewijsmiddel zal dan ook vooral worden ingezet tegen gewone consumenten die content hebben verspreid. Watermerken vormen, evenals veel ander forensisch bewijs, echter geen ideaal bewijs. Dit onderzoek heeft in de verschillende hoofdstukken duidelijk gemaakt dat watermerken evenals ander forensisch bewijs, een lange weg aflegt voordat het als bewijsmiddel in een rechtszaal kan worden ingezet. Op deze weg liggen allerlei risico's ten aanzien van de rechtmatigheid (hoofdstuk 5) en betrouwbaarheid van het watermerk (hoofdstuk 6). De risico's ten aanzien van de rechtmatigheid heeft de rechthebbende zelf in de hand. Dat geldt niet voor de risico's ten aanzien van de betrouwbaarheid van watermerken. Zo blijft er altijd een risico ten aanzien van authenticatie van de licentienemer in het proces van watermerken (inlogprocedure), de techniek zelf en de wijze waarop de rechter uiteindelijk het verslag van het onderzoek begrijpt. Ten aanzien van dit laatste punt is reeds gewezen op de verschillende psychologische valkuilen bij het gebruik van statistiek. Het hiervoor genoemde risico ten aanzien van de authenticatieprocedure en de techniek zelf wordt deels ondervangen door de situatie dat de licentienemer in een procedure aannemelijk zal moeten maken dat de hiervoor bedoelde risico's zijn ingetreden. De bewijspositie van de licentienemer brengt immers met zich mee dat hij niet achterover kan leunen wanneer de rechthebbende het watermerk als bewijsmiddel heeft ingebracht (hoofdstuk 4). Vooral in het civiel recht zal de licentienemer verweer moeten voeren om te voorkomen dat de rechter het feit vaststelt. Om voldoende verweer te kunnen voeren zal een expert nodig zijn. De kosten die dat met zich meebrengt zal bij de licentienemer de vraag oproepen of die kosten de moeite waard zijn. Door een aantrekkelijke schikking voor te stellen kan de rechthebbende het antwoord op de vraag mogelijk sturen. Het watermerk wordt daarmee ook een strategisch middel om de licentienemer te verleiden tot een schikking, waarmee ook de rechthebbende zichzelf veel (handhavings)kosten en moeite bespaart.

[4] Zie o.a. Lessig 1999 die de regulering zoekt in vier modaliteiten: markt, recht, sociale normen en architectuur (techniek).

In de praktijk zal de rechthebbende vanwege de eerder genoemde risico's eerder geneigd zijn het watermerk te gebruiken als start van een onderzoek of als middel om de wederpartij te confronteren in de hoop op een bekentenis (erkenning), op andere, meer en betere bewijsmiddelen of als hulpmiddel om de licentienemer tot een schikking te bewegen. Uit gesprekken met de Belgian Anti-piracy Federation (BAF) blijkt dat mensen bij een confrontatie met bewijsmiddelen snel(ler) bekennen en bereid zijn informatie te verstrekken. Een eventuele bekentenis is juridisch gezien een bewijsstuk dat veel minder risico's met zich meedraagt en als bewijsstuk dus de voorkeur zal hebben van iedere advocaat. Mijn inschatting is dan ook dat het watermerk niet snel als juridisch bewijsmiddel in de rechtszaal zal worden gebruikt. Niettemin geldt evenals bij DNA-bewijs dat partijen zich soms genoodzaakt zullen zien het als bewijs te gebruiken, omdat er verder niet veel bewijs voorhanden is. De waarde van het watermerk is dan ook niet zozeer gelegen in de juridische status van bewijsmiddel als wel in de mogelijkheden die het de rechthebbende kan bieden bij de handhaving van zijn auteursrecht. Bijvoorbeeld als preventiemiddel of als hulpmiddel bij de opsporing of als strategisch middel bij het komen tot een schikking. In al deze gevallen spelen de hoge drempels die in het bewijsrecht gelden ten aanzien van de betrouwbaarheid van het bewijs een veel minder grote rol. De vraag of het watermerk betrouwbaar is zal in deze situaties eerst door licentienemer moeten worden beantwoord. Het is dan de vraag of hij bereid is om kosten te maken om de onbetrouwbaarheid van het watermerk in een procedure aan te tonen. Of dat hij in het licht van die kosten ervoor kiest een schikking te accepteren.

Summary

Watermarks as legal evidence

1. Introduction

This study addresses the question as to whether a non-visible digital watermark that aims at tracing the licensee (hereafter: the watermark) can be an effective means of proof in the Netherlands with respect to the enforcement of copyright on digitally made available photos, music, and video on the internet.[1] In this research the watermark is regarded to be effective when the court considers the alleged fact for which the watermark is brought forward proved. There is a comparative aspect to the research that is presented here, as similarities with and differences between Belgium private and criminal law are also considered.

This research into the technical and legal aspects of watermarking started (2009) from the idea that rights-owners may well be reluctant to make their content digitally available because digital content can be copied easily. At that time, consumer unfriendly physical copy protection was no longer used as a form of Digital Rights Management (henceforth DRM), mostly because of the overtly negative public reception of this type of protection. Whilst this negative response to physical protection clearly demonstrated that consumers do not like to be hindered in any way in the (legal) use of their purchase. Digital watermarks do not hinder consumers in the use of content and in that sense they are to be regarded as a form of DRM with a friendly face.

In recent years, technical capabilities have increased and are now sufficient to be put to commercial use. At the start of my study, I expected that watermarks would develop in the sectors of music, video, and photographs, in part because of the good possibilities of hiding information in these substantial digital files. However, at the end of the research it became clear that watermarking is particularly used for the protection of e-books.

To answer the research question, I researched the way in which watermarking functions, and the role that the watermark is given in the relevant (watermark) literature (section 2). On the basis of substantive (copyright) law, I focus on the role the watermark can play in establishing copyright infringement (section 3). After studying the watermark literature and the material law it soon became clear that a reliable watermark can only demonstrate that the file found on the internet belongs to the licensee. This finding is studied within the framework of legal evidence (section 4). The effectiveness of evidence is evaluated in the light of the fact to be proven by the evidence produced, and the arguments for which that evidence is or can be

[1] As part of a common research programme (IM-PACT) of the Flemish IBBT and the Dutch ICT-Regie in the area of digital media in a cooperation between IBBT-ICTRO (Free University Brussels) an inquiry was done for a technical solution to make available digital content through adding hidden information to content by means of watermarks.

produced. From that perspective, I mainly study the question which arguments parties reasonably can and sometimes ought to put forward in respect of the fact to be proven using the watermark and in which manner the court should assess these arguments. The admissibility (section 5) and the reliability (section 6) of the watermark are the most plausible defences to cause the watermark to lose its effectiveness immediately. After all, an non-admissible watermark cannot be allowed to be used as evidence in the proceedings and the court will not accept an unreliable watermark as evidence. I conclude my summary with a brief discussion of how the watermark could be incorporated in the law and in practice (section 7).

2. Watermarks as technical evidence

In short, digital watermarking is a technique to embed a message in a digital signal or host-object. In this research, I focus on the non-visible watermark that aims to identify the licensee (traitor tracing). In practice, the process of watermarking is that someone buys, for instance, a film through a web shop (licensee) by logging in and providing certain data. These data are then added to the film by means of a watermark. If at a given moment the film is found on the internet the watermark can be read and the licensee be called to account.

In the watermark literature the main focus is on the process of creating, spreading, detecting, and interpreting the watermark. Focus is mainly on using the proper algorithms and keys, as well as on possible attacks on parts of this process and on counter measures against such attacks. The result of looking at watermarks in this way is a probability calculation with respect to the presence of a given watermark and in the end of a probability calculation that the file found on the internet belongs to a certain licensee.

This primary focus on technique from the watermark literature makes sense but is only part of the puzzle when assessing the evidential value of a watermark. The main reason for this is that in the watermark literature the data that go into a watermark are considered to be fixed data. In practice, the watermark as legal evidence consists of two elements.

Firstly, it will have to be shown that the data put into the watermark are reliable (authentication). This means that the defendant or accused in fact is the person who originally purchased the work (file) (hereafter: licensee). For a vast majority of purchasers the right data will normally be known, e.g. because the majority of consumers will provide correct data or because they already have a contractual relationship with their provider (e.g. pay-tv through a provider like KPN or Ziggo). However, it should be noted that a group of purchasers that aims at sharing the files will try to sabotage the input of data, for instance by providing a false name or purchasing through a middleman that offers no recourse, such as a drug addict. This implies that the use of watermarks as legal evidence mainly is to keep honest purchasers honest. An important condition for a watermark to succeed as legal evidence is that the

licensee really is who he says he is. If the rights owner or the public prosecutor can prove that the data are correct the next step is to show the watermark is a reliable technique.

Secondly, it needs to be proven that the watermark is reliable by showing the regularity of the process of creating and interpreting the watermark. It has to become clear that the techniques used can be substantiated in relationship to the aim. Furthermore, the rights owner will have to show that the watermark properties chosen match the desired aim (traitor tracing). Moreover, the choice of embed- and detection mechanism needs to be justified. In virtually all cases one has to consider a myriad of options with different trade-offs. To be able to use the watermark as legal evidence it has to be shown to what degree this interaction has influenced the reliability of the watermark. Finally, attention must be paid to the influence of the most likely attacks on the reliability of the watermark as a technique. For this the literature offers ample discussions and pointers. Another indication of the reliability of a watermark system can be the survival in competitions to hack watermarks. It should be noted, however, that many commercial watermarks keep the system used secret so that both literature and competitions lack relevant information and the other party will have to address an expert to assess the reliability of the watermark used.

3. Watermarks and establishing copyright infringement

Apart from the technical options the effectiveness of the watermark as legal evidence is largely determined by the role that a watermark can play in the context of the law of evidence. Material law determines which role watermarks can play in establishing copyright infringement.

If we look into both Dutch and Belgian substantive (copyright) law we will see that a watermark can play no role when establishing a copyright infringement. The main contribution of a watermark in regard to legal evidence is to produce evidence to establish a link between the licensee and the alleged copyright infringement. The watermark is by no means sufficient to prove any copyright infringement as such.

4. Watermarks as effective means of proof in the law of evidence

Apart from the material law the effectiveness of the watermark as legal evidence is also determined in the context of the law of evidence. When the rights owner argues (and tries to prove) a link between the licensee and an alleged copyright infringement, the most plausible defences of the licensee are in the domain of admissibility (‘illegally obtained”) (section 5) and reliability (section 6) of the watermark. When the court honours one of these defences, it would directly adversely affects the effectiveness of the watermark. A third plausible defence operates in a more indirect way, since it does not directly relates to effectiveness. This is to argue an alternative explanation for the alleged fact. E.g. the argument that although the files contains the licensees data, the file reached the internet by someone else’s acts, e.g. a hack or

a virus. Attractive as this defence may look like it is not easy to argue. Firstly the alternative put forward has to match the established facts and the rights owner should not be able to counter this alternative in any simple way. Secondly the defendant has to prove his argument that there was a hack or that someone else put the file on the internet. In practice it is far from easy, but not impossible, to argue a successful defence as to liability for copyright infringement, on the ground of an alternative explanation for the alleged fact. If only because the licensee may in reality not be the actor.
In general it will not be easy to argue a defence against the watermark as legal evidence. This stems mainly from the fact that the defendant has to substantiate his arguments. To challenge the reliability of the watermark, the defendant will in most cases be in need of an expert. Especially with respect to commercial watermarks, where the literature offers few insights. Using an expert necessitates costs. Apart from costs it will frequently not at all be obvious from the start that the results of the expertise will be in favour of the licensee. The licensee prospect of having to pay full costs of the proceedings in IP-matters and having to pay expert costs makes the watermark an attractive enforcement instrument for rights owners. Using watermarks will enhance the scope for amicable settlements. A settlement may well be the cheapest outcome for both parties as well as staying away from court proceedings. For the rights owner this results in operating the watermark by way of prevention, whereby admissibility and reliability will not immediately be tested (in court). In civil law cases the court can in principle appoint its own expert autonomously or at the request of the parties, but in practice is reluctant to do so for lack of necessity. This is because parties have to argue their case and will or will not bring their own expert. When the rights owner argues the watermark by way of expertise report and the other parties argues a defence the court quite often considers there are sufficient arguments and ground for making a decision. This makes the watermark also a strategic instrument for copyright enforcement, quite distinct from its evidential value.

In a criminal law context the watermark basically functions in the same way. The burden of proof in criminal law is on the public prosecutor, which means – in theory – that the defendant can sit back and wait. In practice the defendant will bring some arguments to his defence to prevent the court from following the public prosecutor blindly. In theory the court itself can investigate the evidence. In practice, however, in a case about a watermark, the court will only do so when there is a conviction that the watermark is inadmissible or unreliable. In that sense the defendant is well advised to argue a defence.

5. Watermarks as admissible evidence

Only those watermarks that the court finds admissible can be used for evidence. Watermarks can be excluded by the court as legal evidence when the watermark is obtained through an infringement of a (fundamental) right of the licensee. To ascertain whether and if so under what circumstances the rights owner acts in breach of the licensees privacy I looked at the privacy rules in the Netherlands and in Belgium.

Both the Dutch and the Belgium Data Protection Act (Dutch: Wet bescherming persoonsgegevens (Wbp); Belgium: Wet met betrekking tot de verwerking van persoonsgegevens (WVP)) are predominantly based on the EC Data Protection Directive and hence have similar conditions for processing personal data in the watermark. Breach of the statutory provisions amounts to a tort in both legal systems. Especially relevant are the circumstances of obtaining, processing and retaining the personal data. The right to privacy in both countries is a functional rather that an absolute right, which means that a balance has to be struck between different parties rights. When the court finds there is a breach of the licensees privacy it has to assess a possible justification thereof. In the case of watermarks the court will have to strike a balance between on the one hand the interest of the licensee in respecting his private life and on the other hand the interest of the rights owner in protecting his intellectual property. When evaluating the seriousness of the breach the degree and intimacy of the information may carry considerable weight. De seriousness of the breach will be of minor importance in the case of watermarks, given the nature and limited scope of intimacy involved. The result is that a breach of the national data protection Acts will normally lead to the conclusion that the evidence is obtained in breach of the law and hence illegally.

In respect of a careful application of these data protection rules the rights owner can align with the “Privacy Principles for Digital Watermarking” published in 2008 by the US Civil Right Center for Democracy & Technology (CDT), where a specific framework is developed to comply with the European Data Protection Directives and their implementation in Dutch and Belgium law. These principles underline the importance of (1) Privacy by design, asking for a data protection perspective right from the start, (2) avoiding the use of directly operable information so that even when the information becomes public it cannot be used directly, (3) user information, (4) limiting access to the reading of watermarks, (5) adequately responding in case of a hack of the watermark algorithm, (6) protecting databases, (7) providing users access and alteration options.

If the court comes to the conclusion that the evidence is obtained in breach of the (privacy) law, the next question to answer is whether this illegality should result in exclusion of the evidence. There seems little reason to do so. According to Dutch private law the Dutch Supreme Court (Hoge Raad) in the case of Achmea/Rijnsberg explicitly held that in private disputes the general social interest of getting to the truth prevails over the interest of excluding evidence. According to the Dutch Supreme Court excluding evidence is only justified when there are additional circumstances. In Belgium the Supreme Court (Hof van Cassatie) since 2008 also holds that in private disputes the use of illegally obtained evidence should only be excluded when (1) the breach or formality carries a nullity, (2) the breach has compromised the reliability of the evidence and (3) the right to a fair trial is breached (Antigoon-doctrine). Unlike the Dutch Hoge Raad the Belgium Hof van Cassatie has not explicitly made clear that the finding of truth in principle carries more weight than the interest

of excluding evidence. Just as the Hoge Raad the Hof van Cassatie created a considerable threshold to exclude illegally obtained evidence.

When the public prosecutor would decide to prosecute the alleged licensee with respect to the watermark the question arises whether or not the public prosecutor is allowed to use evidence that is obtained illegally by the rights owner. As long as there is no government intervention with the illegality both in Dutch and in Belgium criminal law as a rule there is no reason to believe that illegally obtained evidence will be excluded from the evidence. In the case of watermarks the government normally will not be involved in any way with creating watermarks in private parties content. So in general there is not much reason to believe a watermark will be excluded in a criminal case.

To summarize, there are no reasons to believe that watermarks cannot be admitted in evidence. Although the possibility cannot be ruled out that the watermark breaches data protection rules, it will not readily be excluded from providing evidence, partly given the importance of establishing the truth. Thus a defence aimed at excluding the watermark as legal evidence has limited prospects both in Belgium and Dutch private and criminal law.

6. Watermarks as reliable evidence

The question as to when the watermark will be accepted by the court a reliable evidence remains. Both in private and in criminal proceedings the watermark is presented in the form of written evidence. To assess whether the watermark is reliable evidence I examined courts findings in respect of the expertise report provided by the rights owner to accept the watermark as evidence of the fact that the file belongs to the licensee.

Firstly the report should comply with the general demands on (digital) forensic investigations. This implies focus on adequate research questions, method and the way the research is done. This means that the organisation should be able to make the whole process transparent and verifiable. The report will make clear how the quality of the work is guaranteed. The rights owner should be able to present a chain of evidence through a chain of custody. For instance to show that the link of the licensees data and the watermark is correct, or that the file found on the internet in reality is the object-file of the research that carries the watermark in dispute. These demands are not new but should be respected when assessing the watermark as legal evidence in drafting the report.

Secondly the report should make clear whether or not the watermark is reliable evidence. The reliability focusses on two elements. The data put into the watermark should be correct (authentication of the licensee) and the watermarking process should be reliable. This means that the data that were put into the watermark should also be retrievable from it. It also means that the report should not only pay attention to the watermarking technique, but also to the process of authentication and the rationale of its reliability. The most plausible defences of the

defendant with respect to the reliability of the watermark as legal evidence should also be discussed in the report. These defences draw upon the circumstances that the watermark could produce the wrong outcome. Therefore the report will have to evaluate the probabilities of mistakes made in the process of authentication (e.g. wrong name), in the use of the watermarking technique causing a false-positive, and the chance that someone else made available the file using "his" traitor tracing code and without his knowing about this. As well as the implications of the probabilities presented. The report will present information on the measures taken to prevent these course of action. To assess the watermarking technique as reliable the report will also focus on the aim and host-object of the watermark. These findings should make clear whether the watermarking process choses is fit for the object it should protect. Furthermore there should be emphasis on the watermarking technique itself. That means some clarity about the reliability of the algorithms and keys used. It should be made clear how the watermarks are created and detected. Finally the report should discuss the most likely attacks on the chosen watermarking. And if and to what degree that affects the reliability of the watermark as legal evidence in the case that the report is written for.

Thirdly it is of some importance that the court knows how to assess the report. This means that the court has to be aware of the pitfalls in decision-making on evidence especially in respect on the influence of figures and probability-reasoning in the report presented. The court should realise that reading such a report is far from straightforward. As in reports on DNA-evidence, the watermark-report will contain different probability-reasonings. Research into DNA-evidence shows that lawyers find it difficult to appreciate these. Even lawyers that indicated they understood what was in the report quite often failed to summarize the report correctly. This should make the court alert in transforming basically reliable information into the correct decision on the evidence. An incorrect interpretation of the reported research results can indeed lead to misunderstandings about the strength of watermarks as legal evidence. From the rights owners perspective this sort of research indicates a risk in the use of watermarks as legal evidence. Against this background even reliable watermarks can make the watermark ineffective.

Knowledge and experience from the forensic literature should contribute to the alertness in ascertaining facts. Dutch criminal law has a number of judicial errors that have been translated for Dutch private law by De Bock into her criterion for assessing evidence.[2] Alertness is especially important in cases where there is no other evidence that digital evidence. Unlike a DNA-case the source of digital evidence is fragile and the only traces are digital traces. In addition digital traces can be perfectly imitated and counter-evidence is hard to produce, and costly.

[2] See for the criterion of De Bock, section. 4.2.3.1. 'A fact is proven in a private court when the court can reasonably deduce from the available evidence that the fact has happened, and the court cannot just as well deduce from the evidence that the facts as presented and argued by the other party in reality have happened, whereas it is neither the case that evidence is lacking where it could be expected to exist.'

To summarize the court in assessing the evidentiary strength will have to ascertain whether or not the report complies with the general demands for forensic research reports. Furthermore the court has to assess the sufficiency of discussing the reliability of both watermarking as technique and of the personal data incorporated in the watermark. With assessing the evidence the court has to take into account that lawyers find it difficult to appreciate probability-reasonings in reports. This should make the court alert in transforming basically reliable information into the correct decision on the evidence.

7. Final Chord

At the end of this research it is time to take stock. First by answering the questions whether or not the watermark can be fitted into the Dutch legal system. Secondly by answering the question as to whether the watermark can be an effective evidence in Dutch law and if so, under which conditions.

First. Incorporation Test – technical output for legal input.

When deploying a new technology the recurring question is how to fit it in into the law and the legal system. In respect of watermark this research asked the question whether it can be effective evidence in enforcing copyright. Chapters 4 and 5 argue that there is no reason why the watermark could not be admitted as evidence. The nature of the watermark does not present any problems in terms of the undesirability of the technique as such. Ethical questions played a role when introducing DNA(-techniques) as evidence. Such questions appear to be absent in respect of these watermarks.

A next possible question is whether the legislator should give the watermark a separate status in law, comparable to the digital signature. I answer in the negative. Firstly we do not need more and more rules; the legislator is well advised to restrain himself in respect to new legislation. It is better to first wait and see how this object develops in practice (both technically and in law), and then evaluate the need for a separate status in law, for instance by introducing an (evidential) presumption. Secondly there will not be much social consensus for the creation of such a presumption. It is to be noted that copyright enforcement socially seems less important that the safety of and the trust in electronic communication, such as regarding the digital signature. This last consideration partly depends on the application of watermarks. As to watermarks with an authentication aim to support for instance passports or drivers licences a EU Directive comparable to that regulating an electronic signature, is not unthinkable. However, the desirability of such development is a valid question to ask.

Secondly. Preconditions – legal input for technical output.

To respect the effectiveness of the watermark as legal evidence further developments (and use) of watermarks should take account of the privacy of users and the freedom of

information. Furthermore it is important for the use of the watermark as legal evidence to respect accepted forensic principles when evaluating and analysing the watermark. To assess the watermark as legal evidence more scientific evidence of the reliability of the watermark is required, for instance through the developing of (scientific) standards. These elements will be briefly discussed below.

Respect privacy and the freedom of information

Before I concluded that only major breaches of data protection rules lead to exclusion of the watermark as legal evidence in the admissibility test, both in the Netherlands and in Belgium. Furthermore case law hardly puts any sanctions on breach of these rights. From this we may not draw as a conclusion that the design of a system does not bear on the legal consequences. A breach of data protection rules remains a tortious act for which the actor can be held liable by the defendant or the national data protection authority. Moreover it should be pointed out that not taking account with the privacy of the licensee in any way, the court may look upon that as a gross breach of privacy rights, for which exclusion may well be ordered. Finally the court can take account of the breach of privacy in other ways than excluding the evidence, for instance by mitigating damages or reducing a criminal sanction.

The foregoing clarifies that the watermark as legal evidence will not be readily excluded as legal evidence for reason of breach of data protection rules, but that ignoring privacy may well have direct or future negative consequences for the business model that the selling of licences for watermark software in the end also is. One accommodation is to make personal data non-identifiable for the rights owner (introducing so-called Chinese Wall) by using a TTP, and to have a transparent procedure for access by the rights owner or the content provider. Other technical solutions are possible as long as the personal data are protected adequately.

Act according to forensic principles

By using watermarks as legal evidence the rights owner (or the content provider) will have to take account of the prevailing demands of digital forensic evidence right from the start. Such an organisation not only contributes to the reliability of the watermark as legal evidence, but also facilitates to inform parties and the court at a later stage on for instance the applied chain of custody.

Develop (scientific) standards

One important gap to close is that between lawyers and (forensic) experts. From the legal perspective and with a view on reliability and assessing systems it is recommended to invest time and money in developing standards and protocols for evaluation purposes. Such standards are lacking in practice and do not seem to be developed at present. Also in the

watermark literature the need for such development is supported. Although standards are not the only solution, and not having standards does not imply lack of reliability of a watermark system, it would be a boost for legal practice. It would offer a better framework to lawyers before and during legal proceedings. That legal practice is also relevant for watermark scientists may be shown from the fact that in many technical introduction one of the justifications of the (technical) research is found in copyright enforcement.

Finally. Valorisation – the value of watermarks as legal evidence

From the previous research it became clear that a reliable watermark can serve as effective evidence to prove a link between the file found on the internet and the licensee. By answering that question this research project comes to an end. During the last year there is an increasing intention for knowledge valorisation. Following the National Committee Valorisation this can be described as "process of value creation from knowledge, in that knowledge is made fit and/or available for economic and/or social use and is translated into competing products, services, processes and new activities."[3] For this reason I will briefly step outside the domain of my research project and dwell for a moment on the possible value of the watermark as an instrument for copyright enforcement.

The value of a watermark depends on the aim a rights owner has. There is a wide consensus that the answer to the copyright enforcement problem is to be found in a mix of solutions (regulation), of which the use of technical means is one. From the perspective of countering the spreading of copyright protected content the watermark can be used for two important groups. Firstly the watermark can be used to keep those consumers "honest" who do purchase a licence, in creating thresholds by the use of watermarks to discourage further spreading of the content. Watermarks fit in nicely with their motives (e.g. fear for sanctions) to not act illegally. Secondly watermarks can be used to slow down spreading by "the scene", a small group that is technically able and aims at spreading content. The rights owners point then is to keep for instance video away from the internet as long as possible and thus offer movie-theatres and paytv-channels unique content to make available to their customers.

Watermarks as legal evidence will predominantly be directed towards ordinary consumers that have spread content. However watermarks, as much other forensic evidence, are by no means ideal evidence. This research has shown in the different Chapters that watermarks, as any other forensic evidence, has a long way to go before it can be used as evidence in court. On the way there are all sorts of risks in regard of legality (Chapter 5) and reliability of the watermark (Chapter 6). The risks in regard of legality are in control of the rights owner. That is not so for the risks in regard of reliability. We have seen there is always a risk as to the authentication of the licensee in the process of watermarking (log-in procedure), the technique itself and the way the court understands the report in the end. As to this last matter the

[3] See a.o. the report Waardevol - Indicatoren voor Valorisatie van het Rathenau Instituut (Drooge e.a. 2011).

different psychological pitfalls in handling statistics were already mentioned. The aforementioned risk as to the authentication procedure and the technique itself is partly captured in that the licensee will have to show in a proceeding that the risks mentioned indeed materialized. The burden of proof on the licensee implies that he cannot lean back once the rights owner brought the watermark as legal evidence (Chapter 4). Especially in a private law dispute the licensee will have to bring defences to prevent the court "establishing the fact". To bring an adequate defence an expert will be necessary. The costs of that will make the licensee probably think again. By offering an attractive settlement the rights owner can possibly influence the answer to the question. Therewith the watermark also becomes a strategic weapon to bring the licensee to accept a settlement. The rights owner too has a lot to gain.

Because of the risks mentioned the rights owner in practice will be inclined to use the watermark to start up an investigation or as a means to confront the other party in the hope of getting a confession (recognition), or of obtaining other, more and better evidence, or as a means to bring the other party to a settlement. A discussion with the Belgian Anti-piracy Federation (BAF) showed that people confronted with evidence are more quickly "confess" and more easily are prepared to provide information. A possible confession is legally seen evidence that carries less risk and that will prevail in any legal argument. In my opinion the watermark will not readily be used as legal evidence in court proceedings. Nevertheless, as with DNA-evidence, parties will sometimes feel compelled to use it as evidence if only for lack of any other evidence. Thus the value of the watermark is not so much derived from its legal status as evidence in court as in the options it provides for a rights owner to enforce his copyright. For instance as a means of prevention or investigation or as a strategic argument in reaching a settlement. In all these cases the high thresholds in the law of evidence as to the reliability of the evidence are of less importance. In all these situations the question whether the watermark is reliable will first have to be answered by the licensee. It is up to him to decide whether it is worthwhile to incur costs to show the unreliability of the watermark in a court proceeding. Or that this prospect makes him opt for a settlement.

Lijst van gebruikte afkortingen

AA	Ars Aequi (tijdschrift)
A.C.	Arr. Cass. (Arresten van het Hof van Cassatie)
ACTA	Anti-Counterfeiting Trade Agreement
AE	Arnoud Engelfriet (blog.iusmentis.com)
AMI	Tijdschrift voor Auteurs- Media- en Informatierecht
Arbh.	Arbeidshof
Aw	Auteurswet
BAF	Belgian Anti-piracy Federation
BE	België
BIE	Bijblad Industriële Eigendom/ Berichten Industriële Eigendom
BREIN	Bescherming Rechten Entertainment Industrie Nederland
BS	Belgisch Staatsblad
BW	Burgerlijk Wetboek
Cass.	Hof van Cassatie
CBP	College Bescherming Persoonsgegevens
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
Corr.	Correctionele rechtbank
CR	Computerrecht
DAOR	Le droit des affaires – Het ondernemingsrecht
DD	Delikt en delinkwent
EG	Europese Gemeenschap
EIPR	European Intellectual Property Review
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
E&R	Expertise en Recht
Gw	Grondwet
GwH	Grondwettelijk Hof
Handvest EU	Handvest van de grondrechten van de Europese Unie
HR	Hoge Raad
HvJ EG	Hof van Justitie der Europese Gemeenschappen
HvJ EU	Hof van Justitie der Europese Unie
IE	Intellectuele Eigendom
IEEE	Institute of Electrical and Electronics Engineers
IEF	IE-forum (www.ie-forum.nl)
IEFBE	IE-forum (www.ie-forum.be)
IER	Intellectuele Eigendom en Reclamerecht
Ing. Cons	ConsL'ingénieur-conseil: revue technique et juridique des droits intellectuels
IRDI	Droits intellectuels/Intellectuele rechten
JA	Jurisprudentie Aansprakelijkheid
JAR	Jurisprudentie Arbeidsrecht

JBPr	Jurisprudentie Burgerlijk Procesrecht
JIN	Jurisprudentie in Nederland
JLMB	Revue de jurisprudence de Liège, Mons et Bruxelles
JOR	Jurisprudentie Onderneming & Recht
JT	Journal des tribunaux
JTT	Journal des tribunaux du travail
MvT	Memorie van Toelichting
NC	Nullum Crimen: Tijdschrift voor straf- en strafprocesrecht
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
NjW	Nieuw juridisch weekblad
NL	Nederland
OM	Openbaar Ministerie
Pas.	Pasicrisie belge
PbEG	Publicatieblad der Europese Gemeenschappen
PSPB	Personality & Social Psychology Bulletin
R&R	Rechtsfilosofie & Rechtstheorie
RABG	Rechtspraak Antwerpen Brussel Gent
RCJB	Revue critique de jurisprudence belge
RDPC	Revue de droit pénal et de criminologie
RDTI	Revue du droit des technologies de l'information
Rl	Europese richtlijn
RUN	Radboud University Nijmegen
Rv	Wetboek van Burgerlijke Rechtsvordering
RW	Rechtskundig Weekblad
SEO	Stichting voor Economisch onderzoek
TCR	Tijdschrift voor Civiele Rechtspleging
TTP	Thrusted Third Party
Trb.	Tractatenblad
TSR	Tijdschrift voor sociaal recht
TRIPs	Trade-related Aspects of Intellectual Property Rights
TvPP	Tijdschrift voor de Procespraktijk
TvS	Tijdschrift voor Strafrecht
UVRM	Universele Verklaring van de Rechten van de Mens
VUE	Verdrag betreffende de Europese Unie
Vo.	Europese Verordening
VUB	Vrije Universiteit Brussel
WEBV	Wet elektronisch bestuurlijk verkeer
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Literatuurlijst

Aben 2010a – D.J.C. Aben, 'Ad fundum', E&R 2010-3, p. 85.

Aben 2010b – D.J.C. Aben, 'De facto', *RMThemis* 2010-6, p. 223-232.

Aben 2011 – D.J.C. Aben, Waarom Rassin dit keer geen gelijk heeft. Reactie op E.G.C. Rassin, 'Vijf jaar tunnelvisiecommotie: het moet niet gekker worden', RM Themis 2010-5/6, RM Themis 2011/2, p. 35-36.

Adams 2011 – M. Adams, 'Wat de rechtsvergelijking vermag. Over onderzoeksdesign', AA 2011, p. 192-201.

Allemeersch & Schollen 2002 – B. Allemeersch & P. Schollen, 'Behoorlijk bewijs in burgerlijke zaken over de geoorloofdheidsvereiste in het burgerlijk bewijsrecht', *RW* 2002-2003, nr, 2, pp. 41-60.

Allemeersch 2007 – B. Allemeersch, *Taakverdeling in het burgerlijk proces*, Antwerpen: Intersentia, 2007.

Allemeersch 2009 – B. Allemeersch, De naakte Grijsaard. Over de rechter en zijn persoonlijke kennis(sen), Openingsrede ter gelegenheid van de plechtige openingszitting van het 119de werkingsjaar van het Vlaams Pleitgenootschap bij de Balie te Brussel, uitgesproken op donderdag 26 november 2009. Online: http://www.vpgbrussel.be/UserFiles/file/openingsrede%202009.pdf

Allemeersch & Ryelandt 2012 – B. Allemeersch en S. Ryelandt, 'Licéité de la preuve en matière civile: un clone pour Antigoon', JT 2012, p.165-174.

Allemeersch & Van Orshoven 2011 – B. Allemeersch, P. van Orshoven, 'Gerechtelijk recht, Tussen gelijk hebben en gelijk krijgen. Enkele hete hangijzers van het burgerlijk procesrecht anno 2011' in *Recht in beweging, 18de VRG-Alumnidag*, Antwerpen: Maklu 2011, p. 69-92.

Altheide & Carvey 2011 – C. Altheide & H. Carvey Digital, *Forensics with Open Source Tools*, Syngress 2011, Elsevier 2011.

Ancel 1971 – M. Ancel, Utilité et méthodes du droit comparé, Eléments d'introduction générale à l'étude comparative des droits, Editions Ides et Calendes, Neuchâtel 1971.

Anderson 1996 – R.J. Anderson, 'Stretching the Limits of Steganography', in: R. Anderson, eds, *Information Hiding*, volume 1174 of Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1996. (pp. 39-48). Information hiding: First international workshop, Isaac Newton Institute, Cambridge, England, 30 May – 1 June 1996: http://www.informatik.uni-trier.de/~ley/db/conf/ih/ih96.html

Anderson, Schum, Twining 2005 – T. J. Anderson, D.A. Schum & W.L. Twining, 'Analysis of Evidence'(2nd edition), Cambridge: Cambridge University Press, 2005.

Arlan 2011 – H. Arlan, 'Rapport zaak CEAS 2007/31, quis custodiet ipsos custodes, NJB 2011, p. 748-749.

Arnold e.a. 2014 – M.A. Arnold, E. Darmon, S. Dejean, T. Pénard, 'Graduated Response Policy and the Behavior of Digital Pirates: Evidence from the French Three-Strike (Hadopi) Law', SSRN, 16 januari 2014: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2380522&download=yes

Arnou 1986 – P. Arnou, 'Het gezagde van gewijsde van de vrijspraak of buitenvervolgingstelling voor de burgerlijke rechter', in X (ed.), *Strafprocesrecht voor rechtspractici*, Leuven: Acco 1986, (pp. 163-190).

Asser 1991 – W.D.H. Asser, *Grenzen aan de waarheidsvinding in burgerlijke zaken. Heiligt het doel de bewijsmiddelen?*, Nederlandse Vereniging voor Procesrecht, Deventer: Kluwer 1991.

Asser 1999 – W.D.H. Asser, 'Bewijsrechtelijke aspecten van privacy en verzekering', *Verkeersrecht* 1999-1, p. 1-4.

Asser 2005 – E.M. Korthals Altes, H.A. Groen, *Asser procesrecht; deel 7: Cassatie in burgerlijke zaken* (Veegens), Deventer: Kluwer 2005.

Asser 2013 – W.D.H. Asser, *Asser Procesrecht Deel 3, Bewijs*, Deventer: Kluwer 2013.

Asser, Groen & Vranken 2003 – W.D.H. Asser, H.A. Groen en J.B.M. Vranken, m.m.v. I.N. Tzankova, *Een nieuwe balans. Interimrapport Fundamentele herbezinning Nederlands burgerlijk procesrecht*, Den Haag: Boom Juridische uitgevers 2003.

Asser, Groen & Vranken 2006 – W.D.H. Asser, H.A. Groen en J.B.M. Vranken, m.m.v. I.N. Tzankova, *Uitgebalanceerd. Eindrapport Fundamentele herbezinning Nederlands burgerlijk procesrecht*, Den Haag: Boom Juridische uitgevers 2006.

Asser, Nijboer & Schuurmans 2010 – W.D.H. Asser, J.F. Nijboer, Y.E. Schuurmans, *Bewijsrecht: het bewijs geregeld?*, pre-advies voor Nederlandse Vereniging voor Rechtsvergelijking over preadviezen 2010.

Asser-Scholten 1974 – P. Scholten, *Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht. Algemeen deel*, Zwolle: W.E.J. Tjeenk Willink 1974.

Baarsma & Van Buiren (2010) – B. Baarsma & K. van Buiren (2010), 'Marktafscherming bij forensisch onderzoek'. Economisch-Statistische Berichten, 95(4599), p. 758-761.

Barendrecht 1992 – J.M. Barendrecht, *Recht als model van rechtvaardigheid*, Den Haag: Kluwer 1992.

Barni 2003a – M. Barni, 'What is the future for watermarking? (part I)', IEEE Signal Processing Magazine, vol. 20, issue 5, pp. 55-59, September 2003.

Barni 2003b – M. Barni, 'What is the future for watermarking? (part II)', IEEE Signal Processing Magazine, vol. 20, issue 6, pp. 53-59, November 2003.

Bechtold 2002 – S. Bechtold, *Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Managements*, C.H. Beck, München 2002

Beecher-Monas 2007 – E. Beecher-Monas, *Evaluating Scientific Evidence. An Interdisciplinary Framework for Intellectual Due Process*, New York: Cambridge University Press 2007.

Beenders 2010 – Beenders, *Burgerlijke rechtsvordering, Serie Tekst en Commentaar*, Kluwer 2010.

Beernaert 2005 – M. Beernaert, 'La fin du régime d'exclusion systématique des preuves illicitement recueillies par les organes chargés de l'enquête et des poursuites', JLMB 2005, p. 1104. Annotatie onder Cass. 2 maart 2005.

Beltzer 2008 – R. Beltzer, Boekbeschouwingen: 'Opsporing en sanctionering in het strafrecht en in het arbeidsrecht – het onvergelijkbare vergeleken', *Rechtsgeleerd Magazijn THEMIS* 2008-4, p. 177-180.

Berneman 2004 – S. Berneman, 'Sanctionering van onrechtmatig verkregen bewijsmateriaal: een inleiding tot het Antigoonarrest van 14 oktober 2003', T. Strafr. 2004, (pp. 2-39). Pre-advies voor de Vereniging voor de vergelijkende studie van het recht van België en Nederland 2003.

Berneman 2005 – S. Berneman, 'Is het ontmaskeren van een dief een schending van de privacy waard?' *RABG* 2005, 1161, annotatie onder Cass. 2 maart 2005

Bex, Prakken & Verheij – F.J. Bex, H. Prakken & B. Verheij, 'Formalising argumentative story–based analysis of evidence. Proceedings of the 11th International Conference on Artificial Intelligence and Law, 1-10, New York: ACM Press, 2007. Online: http://www.cs.uu.nl/research/projects/evidence/publications/ICAIL2007BexF.pdf

Bex & Verheij 2010 – F. Bex & B. Verheij, 'Het onderbouwen van een feitelijk oordeel in een strafzaak' In: P.J. van Koppen, H. Merckelbach, M. Jelicic & J.W. de Keijser (red.), Reizen met mijn rechter: Psychologie van het recht (pp. 965-982). Deventer: Kluwer. Online: http://www.ai.rug.nl/~verheij/publications/pdf/reizen2010.pdf

Bhoedjang 2008 – R. Bhoedjang, 'Digitaal sporenonderzoek', in: A.P.A. Broeders & E.R. Muller (Red.), *Forensische wetenschap*, Deventer: Kluwer 2008, pp. 373-398.

Bleichrodt 2003 – F.W. Bleichrodt, 'Onrechtmatig verkregen bewijs afkomstig van derden', in: M.S. Groenhuijsen en J.B.H.M. Simmelink (red.), *Glijdende schalen* (liber amicorum J. de Hullu), Nijmegen: Wolf Legal Publishers 2003

Bleichrodt 2010 – F.W. Bleichrodt, *Over burger en opsporing* (oratie Rotterdam), Kluwer 2010.

Blomberge & Michiels 1997 – A.B. Blomberg en F.C.M.A. Michiels, 1997, *Handhaven met effect*, 's-Gravenhage 1997.

Boddington, Hobbs & Mann 2008 – R. Boddington, V.J. Hobbs, G. Mann, 'Validating digital evidence for legal argument'. In: 6th Australian Digital Forensics Conference, 1 - 3 December, Perth. (p. 6) Online: http://researchrepository.murdoch.edu.au/1878/

Boek & Visser 2005 – J.L.M. Boek en R.A. Visser, *Handhaven: eerst kiezen, dan doen. Spanningsvelden in de handhaving*, Expertisecentrum Rechtshandhaving Ministerie van Justitie, 2005.

Bollen 2006 – M. Bollen, *Tunnelvisie als bedrijfsrisico*, Deventer: Kluwer 2006

Boularbah 2008 – H. Boularbah, 'Présentation générale et application dans le temps de la loi du 15 mai 2007 modifiant le Code judiciaire en ce qui concerne l'expertise et rétablissant un article 509quater dans le Code pénal' in: H. Boularbah, Le nouveau droit de l'expertise judiciaire en pratique. Brussel: Larcier 2008.

Boneh & Shaw 1998 – D. Boneh & J. Shaw: 'Collusion-secure fingerprinting for digital data', *IEEE* Transactions on Information Theory, Vol. 44, No. 5, September 1998

Borgesius 2011 – F.J. Zuiderveen Borgesius, 'De nieuwe cookieregels: alwetende bedrijven en onwetende internetgebruikers?' *P&I* 2011, nr. 1, p. 2-11.

Borgers & Kristen 1999 – M.J. Borgers & F.G.H. Kristen, Bewijsrisico, bewijslast en bewijsvoeringslast in het strafproces, *AA* 1999, pp. 886-877.

Borgers & Van Boom 2005 – M.J. Borgers en W.H. van Boom, *De rekenende rechter. Van 'Iudex Non Calculat' naar actieve cijferaar?* Den Haag: BJU 2005.

Borgers 2012 – M.J. Borgers, 'Boekbespreking' (bespreking van F.W. Bleichrodt, Over burgers en opsporing (oratie Rotterdam)), DD 2012/37, p. 406-413.

Bosse 2003 (diss.) – C. Bosse, Bewijslastverdeling in het Nederlandse en Belgische arbeidsrecht (diss. Tilburg), Deventer 2003

Brants, Mevis & Prakken 2001 – C.H. Brants, P.A.M. Mevis & E. Prakken, 'Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw', in: idem (red.), *Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw*, Antwerpen-Groningen: Intersentia Rechtswetenschappen 2001, p. 1-21.

Brants, Mevis, Prakken, Reijntjes 2003 – C.H. Brants, P.A.M. Mevis, E. Prakken, J.M. Reijntjes, 'Op zoek naar grondslagen', in: idem (red.), *Op zoek naar grondslagen. Strafvordering 2001 ter discussie*, Den Haag: Boom Juridische Uitgevers 2003, p. 1-27.

Brinkhoff 2008 – S. Brinkhoff, 'Burgeropsporing' in: congresbundel *De burger als opspoorder*, OM congres 2008

Brinkhoff 2014 (diss.) – S. Brinkhoff, *Startinformatie in het strafrecht*, (dissertatie: Nijmegen) Deventer: Wolters Kluwer 2014.

Brison & Vanhees 2012 – F. Brison, H. Vanhees (red.), Huldeboek Jan Corbet - De Belgische Auteurswet Artikelsgewijze commentaar, Brussel: Larcier 2012.

Broeders 2002 - A.P.A. Broeders, 'Daubers en Saks: het einde van de klassieke identificatiecriminalistiek', *NJB* 2002, 77/36, pp. 1786-1798.

Broeders 2005 - A.P.A. Broeders, *Ontwikkelingen in de criminalistiek. Van vingerspoor tot DNA-profiel - van zekerheid naar waarschijnlijkheid* (oratie Leiden), Den Haag: Boom Juridische uitgevers, 2005.

Broeders & Muller 2008 – A.P.A. Broeders & E.R. Muller (Red.), *Forensische wetenschap*, Deventer: Kluwer 2008.

Broeders 2010 A – A.P.A. Broeders, Het forensisch tekort (afscheidsrede UM). http://www.maastrichtuniversity.nl/web/Main1/Pers/OratiesEnRedes2011.htm

Broeders 2010 B – A.P.A. Broeders, 'Een pleidooi voor toetsbaar deskundigenonderzoek', EeR 2010/4, p. 113-115.

Boorsma 2005 – J. Boorsma, 'Doofblind strafrecht.Tunnelvisie in grote strafzaken, Proces 2005/2, p. 58-65.

Brouwer 2005 – J.G. Brouwer (red.), *Wat maakt een goed jurist?*, Den Haag: Boom Juridische uitgevers 2005.

Brouwer 2008 – H. Brouwer, 'De betrokken burger' in: congresbundel *De burger als opspoorder*, OM congres 2008.

Bruggeman e.a. 2009 – W. Bruggeman, E. De Wree, J. Goethals, P. Ponsaers, P. Van Calster, T. Vander Beken, G. Vermeulen, *Van pionier naar onmisbaar. Over 30 jaar Panopticon*, Antwerpen/Apeldoorn: Maklu, 2009.

Bruinsma 2003 – F. Bruinsma, *Dutch Law in Action*, Nijmegen: Ars Aequi Libri 2003.

Buruma 2008 – Y. Buruma, 'Burger in de dramdemocratie' in: congresbundel *De burger als opspoorder*, OM congres 2008.

Buruma 2009 – Y. Buruma, 'Betrouwbaar bewijs'. Delikt en Delinkwent, 39(4), p. 303-324.

Buruma 2010 – Y. Buruma, 'Ongemakkelijke lessen van Lucia'. *Delikt en Delinkwent*, 42(6), p. 689-706.

Buruma 2011 – Y. Buruma, *Geen blad voor de mond, Strafrechtspraak in Nederland*, Amsterdam: Uitgeverij Bert Bakker 2011.

Van Buskirk & Liu 2006 – E. Van Buskirk, & V.T. Liu, 'Digital evidence: Challenging the presumption of reliability', Journal of Digital Forensic Practice, 1(1), p. 19-26.

Cano e.a 2005 – P. Cano, E. Batlle, E. Gomez, L. de C.T.Gomes and M. Bonnet
'Audio Fingerprinting: Concepts And Applications' (ch. 17), Studies in Computational Intelligence (SCI) 2, Springer-Verlag: Berlin Heidelberg 2005, pp. 233-245 .

Capelle & Van Laethem – J. Capelle & W. van Laethem, *Het statuut van de privé-detective*, Brussel: Uitgeverij Politeia 1997.

Caronni 1993 – G. Caronni, 'Ermitteln unauthorisierter Verteiler von maschinenlesbaren Daten,' *Technical report*, ETH Zürich, Switzerland. Augustus, 1993

Casey 2010 – E. Casey, Handbook of Digital Forensics and Investigation, Elsevier Academic Press 2010.

Casey 2011 – E. Casey, Digital evidence and computer crime: Forensics science, computers and the Internet (3rd ed.). Amsterdam, The Netherlands: Elsevier Academic Press 2011.

Castermans 2007 – M. Castermans, *De hervorming van het deskundigenonderzoek*, Gent, Story Publishers, 2007.

Cattoir 2013 – B. Cattoir, *Burgerlijk bewijsrecht*, Mechelen: Kluwer 2013.

Cayre, Fontaine & Furon 2005 - F. Cayre, C. Fontaine, and T. Furon. 'Watermarking security: theory and practice'. IEEE Transactions on Signal Processing, 53(10), October 2005. Online: http://hal.inria.fr/docs/00/08/80/06/PDF/CayreFontaineFuronCover.pdf

CBPL 2011 – Rapport van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), 6 juli 2011 (aanbevelingen in het kader van een arbeidsrelatie).

Charpentier e.a. 2011 – A. Charpentier, C. Fontaine, T. Furon & I. Cox, 'An Asymmetric Fingerprinting Scheme based on Tardos Codes', in: T. Filler, T. PevnY, S.Carver, A, Ker (Eds), *Information Hiding: 13th International Conference*, IH 2011, Prague, Czech Republic, May 18-20, 2011, Springer-Verlag Berlin, Heidelberg ©2011, p. 43-58.

Chavannes 2013 – R.D. Chavannes, 'Belangenafweging in het informatierecht: het arrest Scarlet/SABAM en de botsing tussen auteursrecht en ondernemingsvrijheid, uitingsvrijheid en privacy', in: 25 jaar *Mediaforum. Een vooruitblik door de achteruitkijkspiegel*, Amsterdam: Otto Cramwinckel 2013.

Choi e.a. 2003 – Jae-Gwi Choi, Kouichi Sakurai, & Ji-Hwan Park, 'Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party'. Conference: Applied Cryptography and Network Security, First International Conference, ACNS 2003. Kunming, China, October 16-19, 2003, Proceedings.

Clark 1996 – Ch. Clark, 'The Answer to the Machine is in the Machine', in Hugenholtz 1996, p. 139 t/m 146.

Cleiren 2001 – C.P.M. Cleiren, 'Waarheid in het strafproces: niet tot elke prijs', in: C.P.M. Cleiren, R.H. de Bock & C.J.M. Klaassen, *Het procesrecht en de waarheidsvinding, preadviezen voor de Nederlandse Vereniging voor Procesrecht*, Den Haag: Boom Juridische Uitgevers 2001, p. 9-31.

Cleiren, De Bock & Klaassen 2001 – C.P.M. Cleiren, R.H. de Bock & C.J.M. Klaassen, *Het procesrecht en de waarheidsvinding, preadviezen voor de Nederlandse Vereniging voor Procesrecht*, Den Haag: Boom Juridische Uitgevers 2001.

Cleiren 2008 – C.P.M. Cleiren, 'Het monopolie op de strafrechtelijke waarheidsvinding
Overwegingen over belang en risico's van private 'deskundigen'-inbreng, Strafblad 2008, p. 272- 285.

Cleiren 1989 – C.P.M. Cleiren, *Beginselen van een goede procesorde* (diss. Leiden), Arnhem: Gouda Quint 1989.

Cleiren 2010 – C.P.M. Cleiren 2010, 'De rechterlijke overtuiging. Een sprong met hindernissen'. *Rechtsgeleerd Magazijn THEMIS*, 2010-5/6, p. 259-267.

Clermont 2012 – K.M. Clermont Death of Paradox: *Perpetrated by Understanding the Standards of Proof*, 2012. SSRN-id1986346-2.

CNRS & UVIGO 2008 – CNRS , UVIGO, Final Report on Fundamental Aspects of Watermarking Schemes, Ecrypt, June 30, 2008. Online: http://www.ecrypt.eu.org/ecrypt1/documents/D.WVL.19.pdf

Commissie-Stolker 2005 – VSNU, *Voorbereiding Onderzoeksbeoordeling Rechtsgeleerdheid. Oordelen over rechten*, (VOR rapport van de 'Commissie Stolker) Den Haag: VSNU 2005. Voor de tekst verwijs ik u naar de website van de vsnu(.nl).

Commissie-Verbeke 2004 – Vlaamse Interuniversitaire Raad (VLIR), *Model voor integrale kwaliteitsevaluatie van het onderzoek in de rechtswetenschappen* (rapport van de 'Commissie Verbeke') 2004. Voor de tekst verwijs ik u naar de website van de vlir(.be).

Cornish e.a. 2003 – W.R. Cornish e.a., 'Procedures and Remedies for Enforcing IPRs: the European *Commission's* Proposed Directive', *EIPR* 2003, p. 447-449.

Corstens 2014 – G.J.M. Corstens, Het Nederlands strafprocesrecht, bewerkt door prof. mr. M.J. Borgers, achtste druk, Deventer: Kluwer 2014.

Coelho e.a. 2009 – M. Coelho, L. Hall, J. Berzowska, P. Maes, 'Pulp-Based Computing: A Framework for Building Computers Out of Paper', in: *In the International Conference on Ubiquitous Computing (Ubicomp) and Proeedings of the 27th international conference extended abstracts on Human factors in computing systems.* Boston, MA, USA: ACM, 2009. Online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.141.6949

Coster 2005 – J.A. Coster, 'De strafrechter, herkening, kans en statistiek' in: M.J. Sjerps en J.A. Coster van Voorhout (red.), Het onzekere bewijs. Gebruik van statistiek en kansrekening in het strafrecht, Kluwer: Deventer 2005, (pp. 185-207).

Couvreur & Rassin 2010 – I. Couvreur. & E. Rassin, 'Tunnelvisie in het opsporingsonderzoek', in P.J. van Koppen, H. Merckelbach, M. Jelicic & J.W. de Keijser (red.), *Reizen met mijn rechter: Psychologie van het recht*, Deventer: Kluwer 2010, p. 203-218.

Cox e.a. 1997 – I.J. Cox, J. Kilian, T. Leighton & T.G. Shamoon, 'Secure spread spectrum watermarking for multimedia', in *Proceedings of the IEEE International Conference on Image Processing*, ICIP '97, volume 6, pages 1673 - 1687, Santa Barbara, California, USA, 1997.

Cox & Linnartz 1998 – I.J. Cox, J-P. M.G. Linnartz, 'Some General Methods for Tampering with Watermarks' Selected Areas of Communications, 16, 4, 587-593, 1998.

Cox e.a. 2008 – I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, 2nd Ed., Morgan Kaufmann 2008.

Craver, Yeo & Yeung 1998 – S. Craver, B-L. Yeo, M. Yeung, 'Technical trials and legal Tribulations', Communications of the A.C.M., vol. 41, no. 7, juli 1998 (pp. 44-54).

Craver e.a. 1998 – S. Craver, N. Memon, B-L. Yeo, and M. Yeung, 'Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications,' *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, May 1998. Online: http://www.cs.arizona.edu/~collberg/Teaching/620/1999/Handouts/hual2.pdf

Craver, Wu & Liu 2001 – S. A. Craver, M. Wu & B. Liu, 'What can we reasonably expect from watermarks?' in 2001 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics, New Paltz, New York, 2001, pp. 223–226.

Crombag 2000 – H.F.M. Crombag, 'Rechters en deskundigen', NJB 2000/33, p. 1659-1665.

Crombag 2006 – H.F.M. Crombag, 'Over tunnelvisie', Trema 2006, 29, p. 273-279

Crombag, De Wijkerslooth & Cohen 1977 – H.F.M. Crombag, J.L. de Wijkerslooth en M.J. Cohen, *Een theorie over rechtelijke beslissingen*, Zwolle: H.D. Tjeenk Willink, 1977.

Crombag, Wagenaar & Van Koppen 1994 - H.F.M. Crombag, W.A. Wagenaar & P.J. Van Koppen, *Dubieuze Zaken: de Psychologie van Strafrechtelijk Bewijs*, 2e druk, Amsterdam: Contact 1994.

Cuevas e.a. 2011 - Cuevas, R., Kryczka, M., Cuevas, A., Kaune, S., Guerrero, C., Rejaie, R. (2011), Is content Publishing in BitTorrent Altruistic or Profit-Driven?, ACM CoNEXT 2010, November 30 - December 3 2010, Philadelphia, USA. Online: http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/11-Cuevas.pdf

De Bock 2011 – R.H. de Bock, *Tussen waarheid en onzekerheid; over het vaststellen van feiten in de civiele procedure*, diss. Tilburg, Deventer: Kluwer 2011.

De Cock Buning 1998 – M. de Cock Buning, *Auteursrecht en informatietechnologie, over de beperkte houdbaarheid van technologiespecifieke regelgeving* (diss. Amsterdam, UvA)., Amsterdam: Otto Cramwinkel, 1998.

De Cock Buning & Van Eek 2009 – M. de Cock Buning en D. van Eek, 'Aansprakelijkheid van derden bij auteursrechtinbreuk' IER oktober 2009, pp. 224-232.

De Corte 2003 – R. De Corte, 'De achterkant van de privacy – Kan het beroep op privacy leiden tot straffeloosheid?', NJW 2003, p. 798-810.

De Jong 1975 – F.J. de Jong, 'De motieven van den rechter en de motivering van het vonnis', *NJB* 1975, p. 541-547.

De Jong 1981 - D.H. de Jong, *De macht van de tenlastelegging in het strafproces*, (diss. Groningen), Arnhem: Gouda Quint 1981

De Jong 1998 – D.H. de Jong, *Een Pyrrusoverwinning van de grondslagleer*, DD 1998, pp. 313-317.

De Groot 1996 – G.R. de Groot, *Het vertalen van juridische informatie*, Preadvies Nederlandse Vereniging voor Rechtsvergelijking, 53, Deventer: Kluwer 1996.

De Groot 2008 – G.R. de Groot, *Het deskundigenadvies in de civiele procedure* (diss. Amsterdam VU), Deventer: Kluwer 2008.

De Groot 2012 – G.R. De Groot, 'De vaststelling van feiten in de civiele procedure'. Bespreking van R.H. de Bock, Tussen waarheid en onzekerheid: over het vaststellen van feiten in de civiele procedure (diss. Tilburg), Deventer: Kluwer 2011, *TCR* 2012, p. 61-64.

De Groot & Elbers 2008 – G. de Groot, N.A. Elbers, *Inschakeling van deskundigen in de rechtspraak. Verslag van een onderzoek naar knelpunten en verbetervoorstellen*, Raad voor de Rechtspraak 2008.

De Groot-Van Leeuwen e.a. 2015 - L. De Groot-van Leeuwen, M. Laemers, I. Sportel. m.m.v. P. Frielink & P.H. Van Kempen, Het vonnis beter uitgelegd? Maatschappelijke effecten van beter motiveren in de strafrechtspraak. Onderzoek uitgevoerd in opdracht van de Raad voor de rechtspraak en beschikbaar gesteld via rechtspraak.nl.

De Hek 2013 - H. de Hek, 'Een beperkte mate van zekerheid. Over de betekenis van accountantsrapporten in de civiele procedure', *TCR* 2013/4, p. 109-116.

De Hert & Gutwirth 2001 - P. De Hert & S. Gutwirth, 'Een theoretische onderbouw voor een legitiem strafproces. Reflecties over procesculturen, de doelstellingen van de straf, de plaats van het strafrecht en de rol van slachtoffers', *Delikt & Delinkwent* 31(10), p. 1048-1087.

De Keijser & Van Koppen 2004 – J.W. de Keijser & P.J. van Koppen. 'Compensatoir straffen: Over de relatie tussen bewijs, overtuiging en straf', in: J.W. de Keijser & H. Elffers (red.). *Het maatschappelijke oordeel van de rechter: De wisselwerking tussen rechter en samenleving*. Den Haag: BJU, pp. 133-183.

De Knijff 2004 – P. De Knijff, 'Bewijsvoering op basis van DNA-profielen en –databases', in: *Justitiële verkenningen, Forensische expertise* 30/1, p. 39-49.

De Knijff 2006 – P. De Knijff, *Meehuilen met de wolven?*, (oratie leiden) Inaugurele rede uitgesproken bij de aanvaarding van het ambt van hoogleraar Populatie- en Evolutiegenetica, 2006. Online: http://www.leidenuniv.nl/nieuwsarchief2/content_docs/deknijffmeehuilen_met_de_wolven1.pdf

De Smet 2005 – B. De Smet, 'Stromingen in het stelsel van nietigheden. Nieuwe criteria voor de uitsluiting van onrechtmatig verkregen bewijs', *T. Strafr.* 2005, pp. 248-266.

De Smet 2009 – B. De Smet, 'De cruciale rol van deskundigen in het strafproces' in W. Bruggeman e.a. (eds.), Van *pionier naar onmisbaar. Over 30 jaar Panopticon*, Antwerpen/Apeldoorn: Maklu, 2009, pp. 219-226.

De Smet 2010 – B. De Smet, 'Enkele problemen rond het deskundigenonderzoek in financiële strafzaken' in: F. Deruyck, M. De Swaef, J. Rozie, M. Rozie, Ph. Traest, R. Verstraeten (eds.), *De wet voorbij* (Liber Amicorum Luc Huybrechts), Intersentia: Antwerpen – Oxford, 2010.

De Waard 1987 – B.W.N. de Waard, *Beginselen van behoorlijke rechtspleging, met name in het administratief procesrecht* (diss. Utrecht), Zwolle: W.E.J. Tjeenk Willink 1987.

De Wolf 2004 – D. De Wolf, 'Nieuwe wending in de rechtspraak betreffende de sanctie bij onrechtmatig verkregen bewijs: het cassatiearrest van 14 oktober 2003', RW 2003-04, p. 1235-1239.

De Wolf 2010 – D. De Wolf, *De rol van de rechter bij de waarheidsvinding in de correctionele procedure* (diss.), Uitgeverij UGA 2010.

Decker 2001 – S. Decker, 'Engineering considerations in commercial watermarking'. *IEEE Communications Magazine*, 39(8) 2001, pp. 128–133.

Deene & Van der Perre 2005 – J. Deene en K. van der Perre, 'Nieuwe Auteurswet. Belang voor de digitale wereld', *NJW* 2005/119, pp. 866-888.

Deene 2010 – J. Deene, 'Intellectuele rechten, kroniek 2010', *NJW* 2011/245, pp. 442-449.

Deene 2011 – J. Deene, 'De rechtsplegingsvergoeding in procedures inzake intellectuele rechten: een sui generis-regime?', *RW* 2010-11, nr. 23 (5 februari 2011), pp. 946-953.

Delaigle, Vleeschouwer & Macq 1998 – J.F. Delaigle, C. De Vleeschouwer & B. Macq, 'Watermarking Algorithm Based on a Human Visual Model', *Signal Processing*, Vol. 66, nr. 3, May 1998, pp. 319–335. Online: http://www.tele.ucl.ac.be/PEOPLE/DELAIGLE/my_publications/Signal_processing98.pdf

Delaigle 2000 (diss.) – J-F Delaigle, Protection of Intellectual Property of Images by
Perceptual Watermarking (diss. Namen), 2000. Online:
http://www.tele.ucl.ac.be/PEOPLE/DELAIGLE/thesis.pdf

Demeersseman – S. Demeersseman, 'Bewijs in strafzaken en privacy' in G. Vermeulen (ed.), *Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen*, Antwerpen: Maklu, 2007.

Den Tonkelaar 2015 – J.D.A. Den Tonkelaar, 'Hoe komen bewoordingen in vonnissen en arresten tot stand'?, AA 2015, p. 594-601, AA20150594.

Derksen 2006 – T. Derksen, *Lucia de B. Reconstructie van een gerechtelijke dwaling*. Diemen: Veen Magazines 2006.

Derksen 2010 – A.A. Derksen, 'Het duivels dilemma van de deskundige of een alledaags probleem?' in *Strafblad* 2010 (afl. 6), pp. 534-556.

Dessing 2012 – M. Dessing, 'CB wil onduidelijkheid over veiligheid verhuren e-boeken wegnemen', *Boekblad(.nl)*, 17 juli 2012.

DFRWS 2001 - Digital Forensic Research Workshop (DFRWS), 'A Road Map for Digital Forensic Research', Augustus 2001. Online: http://www.dfrws.org/2001/dfrws-rm-final.pdf

Dillen 2009 – Dillen, C. 'De psychiaters-deskundigen in strafzaken: de apen van justitie?" in W. Bruggeman e.a. (eds.), *Van pionier naar onmisbaar. Over 30 jaar Panopticon*, Antwerpen/Apeldoorn: Maklu, 2009, p. 202-207.

Dommering 2012 – E.J. Dommering**', '**De zaak scarlet/Sabam. Naar een horizontale integratie van het auteursrecht, *AMI* 2012/2, p. 49-53.

Dondorp 2011 – F.P.A. Dondorp, *Elektronische handtekeningen: juridische waarde en praktisch gebruik*, Den Haag: Sdu Uitgevers, 2011

Dreissen 2007 (diss.) – W.H.B. Dreissen, *Bewijsmotivering in strafzaken* (diss. Maastricht), Den Haag: Boom Juridisch 2007.

Drion 1966 – H. Drion, 'Bewijzen in het recht'. *Rechtsgeleerd Magazijn Themis*, 1966, pp. 406 – 408.

Du Jardin 2003 – J. du Jardin, 'Het recht van verdediging in de rechtspraak van het Hof van Cassatie (1990-2003). Rede uitgesproken door, Procureur-generaal bij het Hof van cassatie, op de plechtige openingszitting van dit Hof op 1 september 2003.
http://www.cassonline.be/uploads/44/redes2003.pdf?PHPSESSID=3c099d4de6a22a3b592d7df314462a4e

Dumortier 2011 – J. Dumortier, 'Alles elektronisch: geschrift, handtekenig, tijdstempels, aangetekende verzending en archivering' in *Recht in beweging*, Antwerpen: Maklu 2011, pp. 217-244.

Dworkin 1986 – R. Dworkin, *Law's Empire*, London: Fontana Press 1986.

Ekelmans 2010 (diss.) – J. Ekelmans, *De exhibitieplicht* (diss. Groningen), Deventer: Kluwer 2010

Ekelmans 2011 – J. Ekelmans, 'Het wetsvoorstel over het recht op inzage, afschrift of uittreksel van bescheiden Geen eindspel, maar een tussenstand', *AA* 2011. p. 349

Elffers 2003 – H. Elffers, "Bij toeval veroordeeld? Statistische analyse van dienstroosterdata in het strafproces", NJB 2003, 78/34 pp. 1812-1814.

Elffers 2004b – H. Elffers, 'Dit zeggen al die getallen eigenlijk! Antwoord aan VanLambalgen en Meester', Trema 2004/7, pp. 293-294.

Englich 2006 – Englich, B., Mussweiler T. & Strack, F. (2006). 'Playing Dice with Criminal Sentences: The Influence of Irrelevant Anchors on Experts' Judicial Decision Making'. *PSPB* 32(2): pp. 188-200.

Embregts 2003 (diss.) – M.C.D. Embregts, *Uitsluitsel over bewijsuitsluiting* (diss. Tilburg), Deventer: Kluwer 2003.

Emes 2011 – A.L.H. Emes, 'Een vervalste handtekening', *NTHR* 2011/3, p. 101-107.

Emster & Verburg 2007 – F.W.H. van den Emster en Mr J.J.I. Verburg, *De Schiedamse parkmoord: Reflectie op een rechterlijke dwaling*, Trema 2005/7, pp. 293-297.

Enneking, Giesen & Rijnhout 2013 – L.F.H, Enneking, I. Giesen & R. Rijnhout, 'Bewijswaardering en psychologische inzichten', in: W.H. van Boom, I. Giesen & A.J. Verheij (red.), *Capita Civilologie. Handboek empirie en privaatrecht*, pp. 1017-1085.

Enschedé 1966 – Ch.J. Enschedé, 'Bewijzen in het strafrecht', *RM-Themis* 1966, pp. 488-518.

Esser 1970 – J. Esser, Vorverständnis und Methodenwahl in der Rechtsfindung, Frankfurt am Main: Rationalitätsgrundlagen richterlicher Entscheidungspraxis, Frankfurt am Main 1972 (3e druk 1970).

Eyadat & Vasikarla 2005 – M. Eyadat, S. Vasikarla, 'Performance evaluation of an incorporated DCT block-based watermarking algorithm with human visual system model', Pattern Recognition Letters, Vol. 26, nr. 10, July 2005, pp. 1405–1411.

Finkelstein & Fairly 1970 – M.O. Finkelstein & W.B. Fairly, 'A Bayesian Approch to Identification Evidence', Harvard Law Review 1970, jrg. 83/3, pp. 489-517.

Franken 2004 – H. Franken, 'Rechtsgeleerdheid in de rij der wetenschappen', *NJB* 2004-28, p.1400-1408.

Franken e.a. 2004 – H. Franken, H.W.K. Kaspersen, A.H. de Wild (Eds.), *Recht en computer*, Deventer: Kluwer 2004.

Franken 2012 - A.A. Franken, 'De zittingsrechter in strafzaken', *DD* 2012-5, pp. 361-368.

Fridrich & Golan 1999 – J. Fridrich and M. Goljan, 'Comparing robustness of watermarking techniques', *Proceedings Electronic Imaging '99, The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, USA, 25-27 January 1999, vol. 3657,* , pp. 214-225. Online: http://dde.binghamton.edu/publications/spie99.doc

Furon & Perez-Freire 2009 – T. Furon, L. Perez-Freire, 'Worst case attack against binary probabilistic traitor tracing codes', *IEEE WIFS* 2009. pp. 46-50.

Garrie & Spernow 2010 – D. B. Garrie & B. Spernow, 'Legally Correct But Technologically Off the Mark', Northwestern Journal of Technology and Intellectual Property, Volume 9, Issue 1 October 2010. Online: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1116&context=njtip

Gellaerts & Häcker 2010 – S.L. Gellaerts & D.W.F. Häcker, 'Marktonderzoek, de onderste steen boven?', *BIE* 2010, pp. 3-12.

Gentleman's Magazine 1779 – Gentleman's Magazine and Historical Chronicle, juli 1779, Volume XLIX, for the Year MDCCLXXXIX, by Sylvanus Urban (pseudonym), Gent, Printed at St. John's Gate, for D. Herny; and fold by F. Newberry, the corner of St. Paul's Church-Yard, Ludgate-Street (p. 331- 376). Het magazine is beschikbaar via google als en via hathitrust: http://babel.hathitrust.org/cgi/pt?id=mdp.39015011429365 (scan van de University of Michigan.

Gerbrandy 1973 – S. Gerbrandy, Kort commentaar op de auteurswet 1912, Haarlem: Bohn, 1973.

Giard 2008 – R.W.M. Giard, 'Mentale misleidingen' (redactioneel), E&R 2008-4, p. 105-107.

Giard 2009 – R.W.M. Giard, Waarheidsvinding: worstelen met wijsheid achteraf, E&R 2009/2. p. 41-45

Giard 2011 – R.W.M. Giard, 'Law and medicine: dokteren aan het recht', WPNR nummer 6912, jrg. 142, 24, pp. 1086-1094.

Giard 2011 - R.W.M. Giard, 'Rechtspraak is een riskante onderneming. De noodzaak van een geïntegreerd normatief kader', E&R 2011/2, pp. 34-40**.**

Giesen 1999 – I. Giesen, 'De bewijswaardering in civiele zaken: vage noties of scherpe normen?', *AA* 1999-9, p. 623-633.

Giesen 2001 (diss.) – I. Giesen, *Bewijs en aansprakelijkheid* (diss. Tilburg), Den Haag: Boom Juridische Uitgevers 2001.

Giesen 2011 – I. Giesen, 'Recht en .. psychologie: over de waarde die psychologische inzichten voor de civilist kunnen hebben', *WPNR* 2011 (6912), p. 1065-1074

Gill 2010 – R. Gill (2010), 'Lies, damned lies, and legal truths' : in L. Mommers, H. Franken, F. van der Klaauw, H. van der Herik, G-J Zwenne (Eds.) *Het binnenste buiten*, liber amicorum Aernout Schmidt (pp. 321-341), Leiden: eLaw@Leiden, pp. 39-50.

Gommer 2007
H. Gommer, 'Onbewuste denkprocessen maken motivering tot noodzaak', *Trema* 2007, pp. 127-134.

Gorlé e.a. 2007 – F. Gorlé, G. Bourgeois, H. Bocken, F. Reyntjens, W. De Bondt, K. Lemmens, *Rechtsvergelijking*, Mechelen: Kluwer, 2007.

Gotzen & Janssens 2009 – F. Gotzen, M.C. Janssens, Wegwijs in het intellectuele eigendomsrecht, Brugge: Vandenbroele, 2009.

Groenhuijsen & Knigge 2001 – M.S. Groenhuijsen & G. Knigge (Eds.), *Afronding en verantwoording*, Deventer: Kluwer. (Onderzoeksproject strafvordering 2001: Eindrapport).

Groenhuijsen 2004 – M.S. Groenhuijsen, 'Bewijsrecht als toetssteen voor de systematiek van een Wetboek van Strafvordering. Pleidooi voor een vrij bewijsstelsel', in: A.H. Klip, A.L. Smeulers, M.W. Wolleswinkel (red.), *KriTies*. Liber amicorum et amicarum voor prof.mr. E. Prakken, Deventer: Kluwer 2004, pp. 147-158.

Groenhuijsen 2008 – M.S. Groenhuijsen, 'Deskundigen in de aanval. Het strafrecht in de verdediging?', DD 2008, afl. 9/65, pp. 929-941. Online: http://arno.uvt.nl/show.cgi?fid=90520

Gross 1987 – S.R. Gross, 'Loss of innocence: Eyewitness identification and proof of guilt.' Journal of Legal Studies, nr. 16, pp. 395-453.

Gross 1996 – S.R. Gross, 'The risks of death: Why erroneous convictions are common in capital cases'. Buffalo Law Review, nr. 44, pp. 469-500.

Grove e.a. 2000 – W.M. Grove, D.H.Zald, B.S.Lebow, B.E.Snitz, & C. Nelson,. 'Clinical versus mechanicalprediction: A metaanalysis', Psychological Assessment 2000/3, pp. 19-30.

Guibault e.a 2007 - L. Guibault, G. Westkamp, T. Rieber-Mohn, B. Hugenholtz, M. Van Eechoud, N. Helberger, L. Steijger, M. Rossini, N. Dufft, P. Bohn, *Study on the Implementation and Effect in Member States' laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*, report to the European Commission, DG Internal Market, February 2007. Online: http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf

Guibault & Mom 2007 – L. Guibault en G.J.H.M. Mom, *Evaluatie van de artikelen 29a en 29b van de Auteurswet 1912*, 2007. Dit onderzoek is uitgevoerd in opdracht van het WODC.

Guthrie, Rachlinski & Wistrich 2001 – C. Guthrie, C., J.J. Rachlinski & A.J. Wistrich, 'Inside the Judicial Mind'. Cornell Law Review 2001, 86(4): p. 777-830. Online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=257634

Guthrie, Rachlinski & Wistrich 2007 – C. Guthrie, J.J. Rachlinski, A.J. Wistrich, 'Blinking on the Bench: How Judges Decide Cases'. Cornell Law Review, Forthcoming; Vanderbilt Public Law Research Paper No. 07-25; Vanderbilt Law and Economics Research Paper, no. 07-32. (pp. 101-141). Online: http://ssrn.com/abstract=1026414

Gutwirth, De Hert & Saelens 2007– S. Gutwirth, P. De Hert, R. Saelens 'Kan privacy nog? Over de voor- en achterkanten van het privacygrondrecht in België, in: M. De Bussher e.a., Kan dit nog? Liber Amicorum Rogier De Corte, 2007.

Haagman & Ghavatas 2005 - D. Haagman & B. Ghavalas, Trojan defence: A forensic view, Digital Investigation Journal, Vol. 2, Issue 1, February 2005, pp. 23–30.

Haardt 1991 – W.L. Haardt, 'Bewijs en balans', in: W.J. van der Nat-Verhage e.a. (red.), Vorm en wezen (Heemskerk-bundel), Utrecht: Lemma 1991.

Hage 2010 – J. Hage, 'Heeft ICT-recht een eigen methode?' in: L. Mommers; H. Franken; J. Van den Herik; F. Van der Klaauw; G-J. Zwenne, Het binnenste buiten Liber amicorum ter gelegenheid van het emiritaat van prof. dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden.

Hagemans 2011 – N. Hagemans, 'ACTA en de Free Trade Agreements. Modern zendingswerk', AMI 2011/4, pp. 136-142.

Hammerstein 2004 – A. Hammerstein, 'Het perspectief van de civiele rechter', in: W.H. van Boom & M.J. Borgers (red.), *De rekenende rechter*, Den Haag: BJu 2004.

Hartung & Kutter 1999 – F. Hartung & M. Kutter, 'Multimedia watermarking techniques. Proceedings IEEE, vol. 87, nr. 7, 1999, pp. 1079–1107. Online: http://www.vis.uky.edu/~cheung/courses/ee639_fall04/readings/procieeehartungkutter.pdf

Harris 2010 – N. Harris, Paper and watermarks, 2010. Hierbij is de online versie gebruikt: http://ihl.enssib.fr/siteihl.php?page=278&aflng=en.

Hastie, Tibshirani & Friedman 2012 – T. Hastie R. Tibshirani and J. Friedman 2012, p. vii. The Elements of Statistical Learning (2nd ed.). Springer 2012. http://statweb.stanford.edu/~tibs/ElemStatLearn/printings/ESLII_print10.pdf

Helberger e.a. 2004 – N. Helberger, N. Dufft, S. van Gompel, K. Kerényi, B. Krings, R. Lambers, C. Orwat en U. Riehm: *Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations*. Published in: INDICARE Project, December 2004, pp. 1-147.

Hendrickx 2006 – F. Hendrickx, 'Privacy op het werk en bewijs van onrechtmatig gedrag: (spookt) Antigoon in het arbeidsrecht?', TSR 2006, p. 663-704.

Herley 2000 – C. Herley, 'Why Watermarking is Nonsense', *IEEE Signal Processing Magazine*, pp. 10-11, September 2000.

Hernandez & Perez-Gonzalez 1999 – J.R. Hernandez, F. Perez-Gonzalez, 'Statistical Analysis of Watermarking Schemes for Copyright Protection of Images', Proceedings of the IEEE, vol. 87, no. 7, July 1999, pp. 1142-1166. Online: http://ece.ut.ac.ir/classpages/F83/ImageProcessing/Papers/WaterMarking/ieee_proc_00771069 _Watermarks.pdf

Hesselink 1999 – M.W. Hesselink, *De redelijkheid en billijkheid in het Europese privaatrecht* (diss. Utrecht), Deventer: Kluwer 1999

Hesselink 2007 – M. Hesselink, 'De Tilburgse inquisitie', *NJB* 2007-33, pp. 2086-2087.

Hidma & Rutgers 2004 – T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004.

Hugenholtz 1989 – P.B. Hugenholtz, *Auteursrecht op informatie* (diss. UvA), Deventer: Kluwer 1989.

Hugenholtz 1996 – P.B. Hugenholtz, *The Future of Copyright in a Digital Environment*, Kluwer Law International, The Hague, 1996.

Hugenholtz 1998 – P.B. Hugenholtz, *Het Internet: het auteursrecht voorbij* (preadvies) Handelingen NJV 1998-I, pp. 197-260.

Hugenholtz 2004 A – P.B. Hugenholtz, 'Een overbodige richtlijn', *IER* 2004-4, pp. 247-248.

Hugenholtz 2004 B – P.B. Hugenholtz 2004, *De toekomst van het auteursrecht: DRM met een vriendelijk gezicht?*, Tekst van lezing gehouden tijdens symposium 'De toekomst van het auteursrecht', georganiseerd door XS4ALL, Amsterdam, 15 oktober 2004. De paginanummering in de voetnoten komt overeen met de gepubliceerde tekst van de lezing door Hugenholtz zelf: http://www.ivir.nl/publicaties/hugenholtz/toekomstauteursrechtDRM.PDF

Hugenholtz 2007 – P.B. Hugenholtz, 'Memento' in de spoorbundel Een eigen oorspronkelijk karakter, uitgeverij *deLex* 2007, pp. 395-406.

Hugenholtz 2008 - P.B. Hugenholtz, 'Toegang tot de bron: het auteursrecht en het internet', AA juli/augustus 2008, p. 581-588.

Hugenholtz 2008b – P.B. Hugenholtz, **'**Open Letter concerning European Commission's 'Intellectual Property Package' aan de President van de Europese Commissie, Dr. José Manuel Barroso. Online: http://www.ivir.nl/news/Open_Letter_EC.pdf.

Hugenholtz 2012 – P.B. Hugenholtz, 'Illegaal uitwisselen van bestanden zal niet verdwijnen', IEF 11104.

Hunter 1978 – D. Hunter, *Papermaking. The History and Technique of an Ancient Craft*, New York, Knopf, 1978 (Dover edition; Dover Publications).

Hutsebaut 1995 – F. Hutsebaut, 'Private opsporing en de bewijsvoering voor de strafrechter' in: L. van Outrive, T. decorte & W. Van Laethem (eds), *Private bewaking en opsoring en de grondrechten van de mensen*, Brussel: Politeia, 1995.

Huybrechts 1995 – L. Huybrechts, 'Het gerechtelijk afluisteren in het Belgisch recht na de nieuwe afluisterwet', Panopticon, 1995, p. 41-58.

Huydecoper 2004 – J.L.R.A. Huydecoper, 'Nous Maintiendrons - de nieuwe 'Richtlijn handhaving', *AMI* 2004/3, pp. 117-123.

Huygen e.a. 2009 – A. Huygen, P. Rutten, S. Huveneers, S. Limonard, J. Poort, J. Leenheer, K. Janssen, N. van Eijk & N. Helberger. *Ups and downs: economische en culturele gevolgen van file sharing voor muziek, film en games* (TNO-rapport34782), Delft: TNO, 2009. Dit onderzoek is uitgevoerd door TNO, SEO en IVIR, in opdracht van de ministeries van OCW, EZ en Justitie.

Jones & Valli – A. Jones & C. Valli, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility*, Burlington: Elsevier 2009.

Kabinetsreactie werkgroep Gerkens 2009 – Kabinetsreactie daarop van 30 oktober 2009, met als kenmerk: DDS 5621176.

Kalker e.a. 1998 – T. Kalker, J-P. Linnartz, G. Depovere, M. Maes, 'On the Reliability of Detecting Electronic Watermarks in Digital Images, Proc. of EUSIPCO'98, Rodos 1998.

Kalker 2001 – T. Kalker. Considerations on watermarking security, IEEE Internationa, Workshop on Multimedia Signal Processing, MMSP'01, pages 201–206, Cannes, France, October 2001.

Kamiya e.a. 2010 - K. Kamiya, K. Naoe, T. Mori & K. Iwamura, 'Development and evaluation of a benchmark tool for digital watermarking', International Journal of Innovative Computing, Information and Control ICIC International, Volume 6, Number 3(B), March 2010 pp. 1305–1312

Katus 2012 – S. Katus, 'Privacy by design ov-chipkaart', *Privacy & compliance* 3 april 2012, p. 42-45.

Katz 1997 – M. Katz, 'Digital watermarks often fail on Web images'. The New York Times, CyberTimes (11 November 1997).

Katzenbeisser & F.A.P Petitcolas 2000 – S. Katzenbeisser & F.A.P Petitcolas (eds), *Information Hiding: techniques for steganography and digital watermarking*, Artech House 2000

Kelk 2010 – C. Kelk, 'De moed des rechters' (column) *AA* 2010, p. 591

Kemna 2004 – A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004

Kent e.a. 2006 - K. Kent, S. Chevalier, T. Grance, & H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*, National Institute of Standards and Technology (NIST), Augustus 2006. Online: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Kerckhoffs 1883 – A. Kerckhoffs, 'La Cryptographie Militaire.'Journal des Sciences Militaires, vol. 9, pp. 5-38. Jan. 1883. Zie online: http://www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf

Kerkmeester en De Mulder 1987, H.O. Kermeester & R.V. de Mulder, 'Statistiek en bewijsrecht', NJB 1987, p. 73-81.

Kerkmeester 2004 – H.O. Kerkmeester, 'Het gebruik van Bayesiaanse statistiek in strafprocessen', in: M.J. Sjerps en J.A. Coster van Voorhout, *Het onzekere bewijs*, Deventer: Kluwer 2004, pp. 99-129.

Kessler 2010 (diss.) – G.C. Kessler 'Judges' Awareness, Understanding, and Application of Digital Evidence', (diss. Fort Lauderdale), Nova Southeastern University.

Keulen e.a. 2010 – B.F. Keulen, H.K. Elzinga, N.J.M. Kwakman, J.A. Nijboer, *Het deskundigenregister in strafzaken. De beoogde werking, mogelijke neveneffecten en risico's*, BJU 2010.

Klaming 2010 – L. L. Klaming, 'The influence of neuroscientific evidence on legal decisionmaking: the effect of presentation mode' (Chapter 5, p.123-132) in: B. van den Berg, L. Klaming (eds.), T*echnologies on the*

stand. Legal and ethical questions in neuroscience and robotics, Technologies on the stand, Nijmegen: Wolf Legal Publishers, 2010.

Klantwaardering Rechtspraak 2011, Regioplan Beleidsonderzoek en Synovate, *Onderzoek onder professionals en justitiabelen bij gerechten*, 2011. Zie online: www.rechtpsraak.nl.

Klijn 2010 – A. Klijn, Redactioneel, Hoe rechters denken: wat Posner ons leert, rechtstreeks 4/2010. Online: http://www.rechtspraak.nl/Organisatie/Publicaties-En-Brochures/rechtstreeks/Documents/Rechtstreek-2010-4.pdf

Knigge 2006 – G. Knigge, 'De schijn van werkelijkheid' in N.J.M. Kwakman, *Partijautonomie of materiële waarheid?*, Den Haag: BJU, 2006 (Afscheidssymposium G. Knigge d.d. 15 september 2005), pp. 33-44.

Koelman 2003 – K.J. Koelman, *Auteursrecht en technische voorzieningen. Juridische en rechtseconomische aspecten van bescherming en technische voorzieningen* (diss. Amsterdam, UvA), IteR-reeks 57, Den Haag: Sdu 2003.

Kok 2012 - S. Kok, 'CB: 'Meer dan de helft nieuwe e-boeken voorzien van watermerkbeveiliging'', Boekblad 1 november 2012 (online-versie).

Kokkini-Iatridou 1988 – D. Kokkini-Iatridou, ed., *Een inleiding tot het rechtsvergelijkende onderzoek [An introduction to comparative law research]*, Deventer: Kluwer 1988.

Komatsu & Tominaga 1988 – N. Komatsu and H. Tominaga; 'Authentication system using concealed image in telematics', in: *Memoirs of the School of Science and Engineering*, Waseda University, 52, 1988, pp. 45-60.

Kooijmans 2010 – T. Kooijmans, 'Bewijzen door de strafrechter', *AA* juli/augustus 2010, pp. 456-465.

Koops & De Hert 2001 – E.J. Koops, & P.J.A. de Hert. 'Privacy is nog steeds een grondrecht'. *AA* 2001, nr. 50, pp. 972-975).

Koops e.a. 2010 – B-J. Koops, R. Leukfeldt, B. Hoogenboom, W. Stol, *Marktwerking in het forensisch onderzoek. Een veldverkenning*. Onderzoek in opdracht van het WODC van het Ministerie van Justitie, 2010. Online: http://wodc.nl/images/1860_Volledige_Tekst_tcm44-303151.pdf

Koops e.a. 2012 – B-J. Koops, R. Leenes, P. de Hert, S. Olislaegers, *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing.* Onderzoek in opdracht van het WODC van het Ministerie van Justitie, 2012. Online: http://www.wodc.nl/onderzoeksdatabase/cloud-computing.aspx?cp=44&cs=6796

Koorn e.a. 2004 – R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen, Privacy Enhancing Technologies, Witboek voor beslissers; uitgave van het Ministerie van BZK, december 2004. Online: www.cbpweb.nl/downloads_technologie/witboek_pet.pdf

Kramer 2006 – X.E. Kramer, 'Over taalkwesties in de Europese Unie en de kunst van het juridisch vertalen', *NIPR*, 2006(3), pp. 254-257.

Krans & Santing-Wubs 2012 – H.B. Krans & A.H. Santing- Wubs, 'Deskundigen in civiele zaken: opties tot vernieuwing' *WPNR* 2012, 6935, pp. 463-469.

Kremer 1999 – M. Kremer, *Onrechtmatig verkregen bewijs in civiele zaken* (diss. Groningen), 1999.

Kutter & Hartung 2000 – M. Kutter & F. Hartung, 'Introduction to Watermarking Techniques' (Ch. 5), in: S. Katzenbeisser & F.A.P Petitcolas (eds), *Information Hiding: techniques for steganography and digital watermarking*, Artech House 2000 (pp. 97- 120).

Kutter & Petitcolas 1999 – M. Kutter and F. A. P. Petitcolas, 'Fair evaluation methods for image watermarking systems', in: *Proceedings Electronic Imaging '99, The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, USA, 25-27 January 1999. pp. 226-239. Online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.37

Kutter, Voloshynovskiy & Herrigel 2000 – M. Kutter, S. Voloshynovskiy & A. Herrigel, 'The Watermark Copy Attack', Procedings of SPIE: Security and Watermarking of Multimedia Contents II, Vol. 3971, San Jose, CA, USA, 2000. Online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.9110

Kuty 2004 – F. Kuty, 'La régle de l'exclusion de la preuve illégale ou irrégulière: de la précision au bouleversement', RCJB 2004, 405, annotatie onder Cass. 14 oktober 2003.

Kuty 2005 – F. Kuty, 'Le droit de la preuve à l'épreuve des juges', *JT 2005*, p. 355 onder Cass. 2 maart 2005.

Kwakman 2010 – N.J.M. Kwakman**,** 'De rol van de deskundige in het Belgische strafproces' hoofdstuk 6 Van Keulen e.a. 2010

Kwakman 2011 A – N.J.M. Kwakman, 'De Wet Deskundige in Strafzaken: een remmende sprong vooruit?', *AA* 2011, 309, pp. 309-317.

Kwakman 2011 B – N.J.M. Kwakman, 'Het nieuwe deskundigenregister; gestolde deskundigheid' *NJB* 2011/31 pp. 2083-2086.

Kwok 2003 – Sai Ho Kwok, Watermark-Based Copyright Protection System Security, Communications of the ACM, October 2003/Vol. 46, no. 10., p. 98-101.

Laenens 2004 – J. Laenes, 'Rechtscultuur en bewijs in civiele zaken', in: *Mélanges Jacques van Compernolle*, Bruxelles: Bruylant 2004, pp. 273-288.

Laenens e.a. 2012 – J. Laenens, K. Broeckx, D. Scheers, P. Thiriar, Handboek gerechtelijk recht, 3e editie, Antwerpen/Cambridge: Intersentia 2012.

Lafaye 2007 – Julien Lafaye, 'An Analysis of Database Watermarking Security', in: *Proceedings of the Third International Symposium on Information Assurance and Security* (IAS 2007), August 29-31, 2007, Manchester, United Kingdom. IEEE Computer Society 2007, pp. 462-467. Online: http://www.informatik.uni-trier.de/~ley/db/conf/IEEEias/IEEEias2007.html#Lafaye07

Langelaar, Setyawan & Lagendijk 2000 – G.C. Langelaar, I. Setyawan & R.L. Lagendijk, Watermarking Digital Image and Video Data. A State of the Art Overview, IEEE, September 2000 (pp. 20-46).

Langelaar 2000 – G.C. Langelaar, *Real-time Watermarking Techniques for Compressed Video Data*, (diss. Delft), Delft University Press 2000. Online: http://repository.tudelft.nl/assets/uuid:e04d072f-7d62-4e88-9d85-c0f3acd0f48c/emc_langelaar_20000201.PDF

Leenheer & Poort 2014 – J. Leenheer & J. Poort, Alleen maar nette mensen: Consumentenonderzoek Downloadgedrag Films. *CentERdata/IViR*, 2014.

Legerstee & Verhoog 2010 – F. Legerstee & E. Verhoog, *Brancheonderzoek Fotografen 2010*. Uitgevoerd in opdracht van FotografenFederatie en Stichting Burafo november 2010 | r2010-0055FL | 9199-MKT. Delft 2010.

Lessig 1999 – L. Lessig, *Code and other laws of cyberspace*, New York: Basic Books, 1999.

Li & Memon 2007 – Q. Li & N. Memon, 'Security Models of Digital Watermarking', Proceeding MCAM'07 Proceedings of the 2007 international conference on Multimedia content analysis and mining pp. 60-64, Berlin: Springer-Verlag, Heidelberg 2007.

Linnartz e.a. 1997 - J.P.M.G. Linnartz, A.C.C. Kalker, G.F. Depovere and R. Beuker, "A reliability model for detection of electronic watermarks in digital images", in: Proc. Benelux Symposium on Communication Theory, Enschede, The Netherlands, 14-16 October 1997, pp. 202-208.

Linnartz 1998 – J.P.M.G. Linnartz, 'The 'Ticket' Concept for Copy Control Based on Embedded Signaling, in: J.-J. Quisquater, Y. Deswarte, C. Meadows & D. Gollmann (eds.), The 5th European Symposium on Research in Computer Security (ESORICS'98), Louvain-la-Neuve, Belgium, September 1998, vol. 1485 of Lecture Notes in Computer Science, Berlin: Springer, (pp. 257-274).
Online: http://www.sps.ele.tue.nl/members/J.P.Linnartz/papers/articles/ticket.pdf

Lodder, Dumortier & Bol 2005 – A.R. Lodder, J. Dumortier, S.H. & Bol, *Het recht rond elektronische hand-tekeningen*, Deventer: Kluwer 2005.

Machiels 1997 – J. Machiels, *Privilegie, censuur en indexen in de Zuidelijke Nederlanden tot aan het begin van de 18de eeuw*, Brussel: Algemeen Rijksarchief te Brussel, 1997 (Educatieve Dossiers, tweede reeks, 15).

Mackor 2010 – Anne Ruth Mackor, ''Wat is waarheid?' De rol van deskundigen bij waarheidsvinding in de strafrechtspraak', *R&R* 2010-1, pp. 52-66.

Macq, Dittman & Delp 2004 – B. Macq, J. Dittmann & E.J. Delp, 'Benchmarking of image watermarking algorithms for digital rights management. Proceedings of the IEEE, 92(6):971–984, June 2004.

Maeyaerts 2012 – P. Maeyaerts in: F. Brison, H. Vanhees (red.), Huldeboek Jan Corbet - De Belgische Auteurswet Artikelsgewijze commentaar, Brussel: Larcier 2012.

Marini e.a 2007 – E. Marini, F. Autrusseau, P. Le Callet, P. Campisi 'Evaluation of standard watermarking techniques': published in: *Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents*, San Jose 2007. Online: http://hal.archives-ouvertes.fr/docs/00/25/06/82/PDF/EI6505_24_finalfinal.pdf

Mason 2012 – S. Mason (eds), *Electronic Evidence*, LexisNexis Butterworths 2012.

Meerwald 2010 (diss.) - Meerwald, 'Digital Watermarking in Visual Multimedia Content' (diss.) University of Salzburg, Salzburg, Austria, June 2010. Online: http://wavela.at/papers/Meerwald10d.pdf

Menting 2015 – M. Menting, (R)Evolutie in het privaatrecht? Enkele beschouwingen over de rol van private regelgeving en de invloed van het EVRM naar aanleiding van HR Achmea/Rijnberg, NTBR 2015/16.

Meulenbroek 2003 – A.J. Meulenbroek, Onderzoek van Biologische sporen en DNA-onderzoek, in: A.P.A. Broeders & E.R. Muller (Red.), *Forensische wetenschap,* Deventer: Kluwer 2008, pp. 205-296.

Meulenbroek 2011 – A.J. Meulenbroek, 'Leidraad en praktische handvatten voor de jurist bij het doorgronden van conclusies forensisch DNA-onderzoek', EeR 2011-3, p. 71.

Michiels & Macq 2006 – B. Michiels, B. Macq, 'Benchmarking of image watermarking algorithms for digital rights management', 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

Miller, Cox & Bloom 1998 – M. L. Miller, I. J. Cox & J. A. Bloom, 'Watermarking in the real world: An application to DVD.', in: J. Dittmann, P. Wohlmacher, P. Horster, & R. Steinmetz (eds.), Multimedia and security. Workshop at ACM Multimedia '98, Bristol, England, pp 71–76, 12–13 September 1998. Online: http://www.cs.ucl.ac.uk/staff/I.Cox/Content/papers/1998/acm98.pdf

Minkenhof en Reijntjes 2009 – J.A. Minkenhof en J.M. Reijntjes, *Minkenhof's Nederlandse Strafvordering*, Kluwer 2009.

Monahan, & Silver 2003 – J. Monahan, & E. Silver, 'Judicial Decision Thresholds for Violence Risk Management', *International Journal of Forensic Mental Health* 2003, 2(1): p. 1-6.

Mougenot 1997 – D. Mougenot, *Droit des obligations: La preuve*, Bruxelles: Larcier, 1997.

Mougenot 2009 – D. Mougenot, 'Notions et principes de la liberté des preuves en droit commercial» in C. Jassogne (ed.), *Traité pratique de droit commercial, titre I: Principes et contrats fondamentaux*, Waterloo, Kluwer, 2009, (95) 106-109.

Mougenot 2011 – D. Mougenout 'La Preuve en matière civile, Chronique de jurisprudence 2002-2010, *JT* 2011, p. 593-606.

Mougenot 2011 – D. Mougenot, 'Antigone face aux juges civils. L'appréciation des preuves recueillies de manière illicite ou déloyale dans les procédures civiles', *DAOR* 2011/240.

Mougenot 2012 – D. Mougenout, *La preuve en droit commercial*, Brussel: die Keure, 2012.

Moulin 2003 – P. Moulin, 'Comments on 'why watermarking is nonsense'', *IEEE Signal Processing Magazine*, vol. 20, issue 6, pp. 57–59, 2003.

Moulin & Koetter 2005 – P. Moulin and R. Koetter, 'Data-hiding codes', in *Proc. IEEE* 2005, pp. 2083-2127.

Neppelenbroek 2013 (diss.) – E.D.C Neppelenbroek, *Softwarebetrekkingen: de auteur, de verkrijger en hun vermogensrechtelijke positie jegens derden*, (diss. Groningen) Boom Juridische uitgevers (BJu).

Nieuwenhuis 1976 – J.H. Nieuwenhuis, 'Legitimatie en heuristiek van het rechterlijk oordeel', *RM Themis* 1976, p. 494-515.

Nieuwenhuis 2007 – J.H. Nieuwenhuis, 'De juristen moeten de vragen stellen, Interview met prof. Hans Nieuwenhuis', in: Philip Fruytier e.a. (red.), *Multidisciplinaire bestudering van de rechtswetenschap* (AA 2007/10, bijzonder nummer), Nijmegen: Ars Aequi Libri 2007, p. 920-925.

Nijboer 2002 – J.F. Nijboer, *Het gekooide denken, over de rol van discipline binnen feitenonderzoek en bewijs in het recht* (oratie Leiden), Leiden: Universiteit Leiden 2002.

Nijboer 2004 – J.F. Nijboer, 'De rol van (forensische) statistiek in het strafrechtelijk feitenonderzoek en bewijs', in W.H. van Boom & M.J. Borgers (red.), *De rekenende rechter*, Den Haag: Boom Juridische Uitgever 2004.

Nijboer 2004 – J.F. Nijboer, 'De rol van expertise in de rechtspraktijk', in: Justitiele verkenningen, Forensische expertise 2004, 30/1, p. 9-19.

Nijboer, Schuurmans & Asser 2010 – W.D.H Asser, J.F. nijboer & Y.E. Schuurmans, *Bewijsrecht: het bewijs geregeld?*, Nijmegen: Wolf Legal Publishers 2010.

Nijboer 2011 – J.F. Nijboer, *Strafrechtelijk bewijsrecht*, Nijmegen: Ars Aequi Libri 2011.

Nikolaides e.a. 2001 – A. Nikolaidis, S. Tsekeridou, A. Tefas and V. Solachidis, 'A survey on watermarking application scenarios and related attacks', Proceedings of 2001, IEEE International Conference on Image Processing (ICIP 2001), Volume: 3, October. 2001, pp. 991-994.

NIST 2004 - National Institute of Standards and Technology (NIST), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, US Departement of Justice, National Institute of Justice (NCJRS) 2004. Online: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Niu e.a 2010 – Y. Niu, M. Kyan, S. Krishnan & Q. Zhang, 'Voyatzis, Nikolaides & Pitas 1998 - G. Voyatzis, N. Nikolaides & I. Pitas, 'Digital watermarking: An overview', in: Proceedings IX European Signal Processing Conference (EUSIPCO), Island of Rhodes, Greece, Sept. 8-11, 1998, pp. 13-16. Online: http://www.wizpia.com/files/paper/12-02-2001/voyatzis98digital.pdf', Signal Image and Video Processing, No. 11760, ISSN: 1863-1703, vol. 4, no. 2, 2010.

Nikolaidis e.a. 2001 – A.Nikolaidis, S.Tsekeridou, A.Tefas & V.Solachidis, 'A survey on watermarking application scenarios and related attacks' in: Proc. of IEEE Int. Conference on Image Processing (ICIP 2001), Thessaloniki, Greece, 7-10 October, 2001.

O'Mara 2009 – S. O'Mara, 'Torturing the Brain: On the Folk Psychology and Folk Neurobiology Motivating. Enhanced and Coercive Interrogation Techniques' Trends in Cognitive Sciences, Vol. 13 (10), 2009.

Oerlemans & Koops 2011 – J.J. Oerlemans & B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *NJB* 2011, p. 1181-1185.

Olieslagers & Van Gompel 2014 – W.Y.J.L. Olieslagers en S.J. Van Gompel, Het proceskostenrisico in IE-zaken. Een empirisch onderzoek naar toepassing van de indicatietarieven, *AMI* 2014 /5, p. 133-138.

Pels 2011 – D. Pels, 'Stilhouden van hacken is einde bedrijf', Dagblad Trouw 06-09-2011. Online: http://www.trouw.nl/tr/nl/5133/Media-technologie/article/detail/2892633/2011/09/06/Stilhouden-van-hacken-is-einde-bedrijf.dhtml

Pennington & Hastie 1993 – N. Pennington, and R. Hastie, 'Reasoning in explanation–based decision making'. Cognition vol. 49:1-2, pp. 123-163. Story model for juror decision making, in: r. hastie, inside the jury.

Pérez-Freire 2008 (diss.) – L. Pérez-Freire, *Digital Watermarking Security* (Diss. University of Vigo), 2008. Online: http://www.gts.tsc.uvigo.es/gpsc/publications/wmark/thesis_lpfreire.pdf

Perrig & Willmott 1998 – A. Perrig & A. Willmott, 'Digital Image Watermarking in the Real World'. Online: www.cs.cmu.edu/~ajw/public/watermark.ps.gz

Petitcolas, Anderson & Kuhn 1999 – F. A. P. Petitcolas, R. J. Anderson & M.G. Kuhn, 'Information Hiding - A Survey', *Proceedings of the IEEE, special issue on protection of multimedia content*, 87 (7), July 1999, pp. 1062-1078. Online: http://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf

Pfitzmann & Waidner 1997 – B. Pfitzmann, M. Waidner, 'Anonymous Fingerprinting', Eurocrypt '97, LNCS 1233, Springer-Verlag, Berlin 1997, p. 88-102.

Pfitzmann & Schunter 1996 – B. Pftizmann & M. Schunter, 'Asymmetric Fingerprinting' in: *Advances in Cryptology EUROCRYPT 96*, vol. 1070 of LNCS, Springer-Verlag 1996, p. 88-102.

Polak 2010 – M.V. Polak, 'So you think you can rank', *AA* maart 2010, p. 180-181.

Poort & Leenheer 2012 – J. Poort en J. Leenheer, Filesharing 2©12. Downloaden in Nederland. IVIR 2012.

Poort 2014 – J. Poort, Tijd voor meer legale popcorn, Auteursrechtdebat 14 oktober 2014, IEF 14277

Posthumus 2005 – F. Posthumus, *Evaluatieonderzoek in de Schiedammer parkmoord*. (Rapport Posthumus) Rapport in opdracht van het College van procureurs-generaal, Den Haag: Openbaar Ministerie 2005.

Prins 2011 – J.E.J. Prins, 'Normering, regulering en rechtshandhaving door technologie: over de implicaties van technoregulering voor het privaatrecht', WPNR (6912), pp. 1075-1085.

Prins, Erkin & Lagendijk 2007 – J.P. Prins, Z. Erkin, R.L. Lagendijk, 'Anonymous Fingerprinting with Robust QIM Watermarking Techniques', EURASIP Journal on Information Security, 2007 (pp. 1-13) http://repository.tudelft.nl/view/ir/uuid%3Af5e4ddb5-8b2a-4f3c-bcad-402ac0191406/

Prinsen 2008 – M. Prinsen, *Forensisch DNA-onderzoek. Een balans tussen opsporing en fundamentele rechten*, (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2008.

Quaedvlieg 1987 – A.A. Quaedvlieg; *Auteursrecht op techniek* (diss. Nijmegen), Zwolle: Tjeenk Willink 1987.

Quaedvlieg 2014 – A.A. Quaedvlieg, 'UsedSoft: Digitiale uitputting tot elke prijs', in: A.S. Hartkamp e.a. (red.), *De invloed van het Europese recht op het Nederlandse privaatrecht* (Serie Onderneming en Recht deel 81-II), Deventer: Kluwer 2014; *IEF* 13987.

Raad voor de Rechtspraak 2011 – BTC MediaTest BV, *Eindrapportage effect 'DE RECHTBANK' op kennis en houding*, 2011

Raat, Heijnen & Malsch 2009 – R. Raat, W.M.M. Heijnen & M. Malsch. 'Zijn rapporten van DNA-deskundigen duidelijk voor juristen?' Themis 2009/4, pp. 157-162.

Rachlinski 2012 – J.J. Rachlinski, 'Judicial Psychology', Rechtstreeks 2012 nr 2, SDU uitgevers (pp. 15-34). Online:http://www.rechtspraak.nl/Organisatie/Publicaties-En-brochures/rechtstreeks/Documents/Rechtstreeks%202012-2.pdf

Raj & Alli 2012 – Y. A. Raj and P. Alli, An Analysis and Overview of Modern Digital Watermarking, American Journal of Applied Sciences, Vol 9, Issue 1, pp. 66-70.

Rapport werkgroep Gerkens 2009 – Werkgroep Gerkens, *Auteursrechtbeleid*, TK2008–2009, 29 838 en 31 766, nr. 19. Herdruk, een herziening van de eerder gepubliceerde rapportage van 17 juni 2009.

Rassin 2007 – E. Rassin, *Waarom ik altijd gelijk heb: Over tunnelvisie*. Schiedam: Scriptum 2007.

Rassin 2008 – E. Rassin, 'Sickesz vs. de Vereniging tegen de Kwakzalverij. Een illustratie van het belang van integratie van de empirische wetenschap in de rechtsgeleerdheid', E&R 2008-1, pp. 3-8.

Rassin 2010 – E. Rassin, 'Vijf jaar tunnelvisiecommotie: het moet niet gekker worden', *RMThemis* 2010-5/6, pp. 206-214.

Rassin 2011 – E. Rassin, 'Nawoord bij reactie D.J.C. Aben', RMThemis 2011/2, p. 37.

Rassin 2012 – E. Rassin, 'Inleiding op 'Judicial psychology' van J.J. Rachlinski', Rechtstreeks 2012 nr 2, SDU uitgevers (pp. 11-14). Online: http://www.rechtspraak.nl/Organisatie/Publicaties-En-Brochures/rechtstreeks/Documents/Rechtstreeks%202012-2.pdf

Reisig 2005 – D. Reisig, *Het aanbod van getuigenbewijs* (diss. Amsterdam, UvA), Overveen 2005.

Renaud 1996 – J.L. Renaud, 'PC industry could delay DVD', *Advanced Television Markets*,issue 47, May 1996.

Rijnsburger & Malsch 2013 – M. Rijnsburger & M. Malsch, '*Toetsing door de rechter van deskundigenbewijs. Is er voldoende tegenspraak?*', E&R 2013-1, p. 1-8.

Ringnalda, Elferink & De Cock Buning 2009 – WODC-rapport, *Auteursrechtinbreuk door P2P filesharing, Regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*, 2009. Dit onderzoek is uitgevoerd in opdracht van het WODC vanwege het CIER (UU) door A. Ringnalda, M. Elferink, M. de Cock Buning.

Roche & Dugelay 1998 – S. Roche & J.-L. Dugelay, 'Image Watermarking Based on the Fractal Transform,' in Workshop on Multimedia Signal Processing, *IEEE*, Los Angeles, California, 7-9 Dec. 1998, pp. 358–363.

Ronse e.a. 1988 – J. Ronse, L. De Wilde, A. Claeys & I. Mallems, *Schade en schadeloostelling*; A.P.R;, Gent: Story-scientia, 1988.

Roosendaal 2013 – A. Roosendaal, *Digital personae and profiles in law*, Wolf Legal Publicers, 2013.

Royakkers 2009 - L.M.M. Royakkers, 'Logica en recht: een onhoudbaar huwelijk', *AA* 2009-1, p. 11-20.

Rozemond 2010 – K. Rozemond, 'Slapende rechters, dwalende rechtspsychologen en het hypothetische karakter van feitelijke oordelen', *R&R* 2010-1, p. 39-51.

Ruanaidh & Pereira 1998 – J.J.K. Ó Ruanaidh and S. Pereira, 'A secure robust digital image watermark', Electronic Imaging: Processing, Printing and Publishing in Colour, SPIE Proceedings, Zürich, Switzerland, May 1998. Online: http://www.fim.uni-

linz.ac.at/lva/Rechtliche_Aspekte/2001SS/Stegano/leseecke/a%20secure%20robust%20digital%20image%20watermark.pdf

Rückert, Hodeĉek & Wenger 2009 – Peter Rückert, S. Hodeĉek, E. Wenger, *Bull's head and mermaid. The History of Paper and Watermarks from the Middle Ages to the Modern Period*, Tübingen: Gulde-Druck GmbH 2009 (Bernstein Project). Online: http://www.bernstein.oeaw.ac.at/twiki/pub/Main/ProjectExhibitions/bernstein_2009_book_en.pdf

Rupley 1996 – S. Rupley, 'What's holding up DVD?' PC Magazine, vol. 15, no. 20, November 19, 1996.

Rutgers 1988 – G. R. Rutgers, R. J. C. Flach, G. J. Boon, *Parlementaire geschiedenis van de nieuwe regeling van het bewijsrecht in burgerlijke zaken*, Deventer: Kluwer 1988

Samyn 2010 – B. Samyn, 'De bewijslast. Rechtsleer getoetst aan tien jaar cassatierechtspraak, deel 2, P&B.

Samyn 2012 – B. Samyn, Privaatrechtelijk bewijs. Een diepgaand en praktisch overzicht, Gent: Story Publishers, 2012.

Sandvliet & Engelfriet 2012 – K.E. Sandvliet en A.P. Engelfriet, Vaststellen van schade bij online Auteursrechtinbreuk, *AMI* 2012/5, pp. 204-209

Saunders 2005 – H.D. Saunders, 'Quantifying Reasonable Doubt: A Proposed Solution to an Equal Protection Problem, *bepress Legal Series, Working Paper, no. 881, 2005*. Gepubliceerd op http://law.bepress.com/expresso/eps/881/

Scheers & Thiriar 2008 – D. Scheers en P. Thiriar, 'Het gerechtelijk recht in de hoogste versnelling', Antwerpen: Intersentia, 2008.

Scheers & Thiriar 2010 – D. Scheers en P. Thiriar, 'Repareer de reparatie! De aanpassingen door de wet van 30 december 2009 inzake het deskundigenonderzoek', RW 2009-10, nr. 34, p. 1410-1427.

Scheltema 1939 – H.J. Scheltema, *Nederlandsch burgerlijk bewijsrecht*, Zwolle: W.E.J. Tjeenk Willink 1939.

Schellekens 2010 – M.H.M. Schellekens, 'Digital watermarks as legal evidence', *Digital Evidence and Electronic Signature Law Review*, vol. 8 (pp. 152-164).

Schermer & Wubben 2011 – B.W. Schermer, M. Wubben, Feiten om te delen. Digitale contentdistributie in Nederland, Consideratie 2011. Online: http://www.considerati.com/uploads/media/Feiten_om_te_Delen.pdf

Schriks 2004 – C.F.J. Schriks, *Het Kopijrecht in de 16e tot de 19e eeuw*, Zutphen: Walburg Pers/Kluwer 2004.

Schuermans 2004a – F. Schuermans, 'De nieuwe cassatierechtspraak inzake de sanctionering van het onrechtmatig verkregen bewijs: doorbraak of bres?', *RAGB* 2003, annotatie onder Cass. 14 oktober 2003 (Antigoon I).

Schuermans 2004b – F. Schuermans, 'Ook de onrechtmatige voertuigzoeking kan dienen als geldig bewijs: het cassatiearrest van 14 oktober 2003, *Viliges* (N) 2004/1, 15, noot onder Cass. 14 oktober 2003 (Antigoon I).

Schuermans 2004c – F. Schuermans, 'Cassatie verfijnt en relativeert de bewijsuitsluitingsregels in strafzaken', *RABG* 2004, 1061, annotatie onder Cass. 23 maart (Antigoon II;).

Schuermans 2005 – F. Schuermans, 'Het bewijs in strafzaken: het Hof van Cassatie en de strafvorderlijke gevolgen van de schending van een grondrecht', *RABG* 2005, 504, annotatie onder Cass. 16 november 2004, P.04.1127.N.

Schuermans 2007 – F. Schuerman, 'Bolletjesslikker ontspringt dans door aanwezigheid camera', De Juristenkrant 2007, 12 september 2007, p. 8.

Schuermans 2010 – F. Schuerman, 'Antigoon-rechtspraak nu definitief in de fase van de rustige vastheid', RABG, 2010/1, pp. 17-24. Annotatie onder EHRM 28 juli 2009 (Lee Davies/België).

Schuermans 2011 – F. Schuerman, 'Na Straatsburg betonneert nu ook Grondwettelijk Hof de Antigoon-rechtspraak', *RABG* 2011/8. Annotatie onder GwH 22 december 2010.

Schum 2001 – D.A. Schum, *The evidential foundations of probabilistic reasoning*, Northwestern University Press 2001.

Schum 2009 – D.A. Schum, 'Studies of the science of evidence in legal education', *AA* 2009/1, p. 68-71.

Schuurmans, Pill & Groothuis 2012 - Y.E. Schuurmans, K. Pill & M.M. Groothuis, 'De rechter op internet', CR 2012/118, pp. 250-260.

Sen Poh & Martin 2009 G. Sen Poh & K.M. Martin, 'Classification Framework for Fair Content, Tracing Protocols', IWDW 2009, LNCS 5703, 2009, p. 252–267.

SEO 2008 – SEO, *De economische omvang van het auteursrecht in Nederland, Een studie op basis van de WIPO-Guide*, 2008. Dit onderzoek is uitgevoerd in opdracht het Ministerie van Economische Zaken door de SEO en uitgevoerd door J. Leenheer, S. Bremer en J. Theeuwes.

Simmelink 2001 – J.B.H.M. Simmelink, 'Bewijsrecht en bewijsmotivering', in Strafvordering 2001, *Het onderzoek ter terechtzitting* (red. M.S. Groenhuijsen, G. Knigge).

Selamat, Yusof, & Sahib 2008 – S.R. Selamat, R. Yusof, S, Sahib, 'Mapping Process of Digital Forensic Investigation Framework', IJCSNS, Vol.8, no.10, October 2008, p. 163-169.

Shannon 1949 – C. E. Shannon, 'Communication Theory of Secrecy Systems', *Bell System Technical Journal*, vol. 28-4, pp. 656-715, 1949, p. 662. Online: http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

Shieh e.a. 2003 – C-S Shieh, H-C Huang, F. Hsingwang, J-S. Pan, 'An Embedding Algorithm for MultipleWatermarks', Journal of information science and engineering, vol. 19, 2003, pp. 281-395. Online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.4116

Sijmonsma 2010 (diss.) – J.R. Sijmonsma, *Het inzagerecht. Artikel 843a van het Wetboek van Burgerlijke Rechtsvordering*, Deventer: Kluwer 2010.

Sjerps & Coster van Voorhout 2005 – M.J. Sjerps en J.A. Coster van Voorhout (red.), Het onzekere bewijs. Gebruik van statistiek en kansrekening in het strafrecht, Kluwer: Deventer 2005.

Sjerps & Kloosterman 2005 – M.J. Sjerps & A.D. Kloosterman, 'De bewijswaarde van forensisch DNA-onderzoek' in: M.J. Sjerps en J.A. Coster van Voorhout (red.), Het onzekere bewijs. Gebruik van statistiek en kansrekening in het strafrecht, Kluwer: Deventer 2005, (pp. 307-340).

Sjerps 2008 – M.J. Sjerps, 'Forensische statistiek en kansrekening', in: A.P.A. Broeders & E.R. Muller (Red.), *Forensische wetenschap*, Deventer: Kluwer 2008, pp. 467-496.

Slattery 2012 – B. Slattery, (December 19, 2008). 'RIAA Stops Suing Individuals: Are We Home Free?'. http://www.pcworld.com/article/155769/riaa_p2p_lawsuits.html. Bevestigd door: http://www.wired.com/business/2008/12/riaa-says-it-pl/.

Sluiter 2011 – P. Sluiter, *Sturen met proceskosten* (diss. Tilburg), Deventer: Kluwer 2011.

Smithuis, Van Ruth & Wieles 2012 – M. Smithuis, E. van Ruth en E. Wieles, 'Kwaliteitsborging van forensisch deskundigen: de complementaire rol van accreditatie en certificering', EeR 2012/6, p. 220-223.

Smits 2008 – P. Smits, *Artikel 6 EVRM en de civiele procedure* (diss. Leiden 1996), 2e druk, Deventer: Kluwer 2008.

Snijders e.a. 2007 – H.J. Snijders, C.J.M. Klaassen, G.J. Meijer, *Nederlands Burgerlijk Procesrecht*, Deventer: Kluwer 2007.

Snijders 1992 – H.J. Snijders , *Op de grens van burgerlijk recht en burgerlijk procesrecht*, Arnhem/Deventer/Zwolle 1992.

Stevens & Koops 2009 – L. Stevens & E.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno'. *DD* 2009/39 (7), pp. 669-696. Online: https://pure.uvt.nl/portal/files/1174484/STEVENS_Koops_opzet_harde_schijf_DD2009_100113.pdf

Stijns 1990 – S. Stijns 'Gedrag en wangedrag der partijen in het burgerlijk geding. Spanningsverhoudingen met de bewijsvoering', RW 1989-1990, nr. 3. p. 1003-1020.

Spoor, Verkade & Visser 2005 – J.H. Spoor, D.W.F. Verkade en D.J.G., *Auteursrecht. Auteursrecht, naburige rechten en databankenrecht*, Deventer: Kluwer 2005

Steinbach & Wolf 2008 – M. Steinebach & P. Wolf, 'On the necessity of finding content before watermark retrieval: Active search strategies for localising watermarked media on the Internet' (Ch. IV), in: Chang-Tsun Li (edt.), *Multimedia Forensics and Security*, IGI Global, Hersbey, USA, 2008.

Steinebach e.a. 2010 – M.Steinebach, P. Wolf 2010 , J-U. Kim, J. Engelhardt, 'Legal Aspects of Watermarking Search Services', 2010. Paper gepresenteerd op 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 6th International ODRL Workshop. Online: http://virtualgoods.org/2010/VirtualGoodsBook2010_162.pdf

Stolker 2011 – C.J.J.M. Stolker, 'Een discipline in transitie. Rechtswetenschappelijk onderzoek na de Commissie Koers. *Recht en Methode in onderzoek en onderwijs*, 1 (1), pp. 13-43.

Storme 1962 – M.L. Storme, *De bewijslast in het Belgisch privaatrecht*, Gent: Story-Scientia, 1962.

Storme 1990 – M.E. Storme, 'De goede Goede trouw in geding en bewijs - De Goede trouw in het geding? De invloed van de goede trouw in het privaat proces- en bewijsrecht, *Rapport voor het 34e Wetenschappelijk Kongres van de Vlaamse Juristenvereniging*, 1990. Ook verschenen in *TPR* 1990 nr. 2, pp. 353-543 (in het extranummer pp. 311-484).

Storme 2001 – M. Storme, 'Het verrichten van rechtshandelingen door middel van nieuwe telecommunicatiemiddelen – de nieuwe wetsbepalingen ingekaderd in de algemene leer van de kennisgeving, *RW* 2001-2002, pp. 1505-1525.

Struik, Van Schelven & Hoorneman 2010 – H. Struik, Peter van Schelven & W.A.J. Hoorneman, *Softwarerecht, Bescherming en gebruik van computerprogrammatuur onder auteursrecht en octrooirecht*, Deventer: Kluwer 2010.

Swanborn 1987 – P.G. Swanborn, *Methoden van sociaal-wetenschappelijk onderzoek*, Meppel: Boom 1987.

Swanson, Kobayashi & Tewfik 1998– M.D. Swanson, M. Kobayashi & A.H. Tewfik, 'Multimedia data-embedding and watermarking technologies,' Proceedings of the IEEE, vol. 86, pp. 1064-1087, June 1998; www.ecpe.nu.ac.th/paisarn/Multimedia/water.pdf

Schwartzenberg 2013 - H.W.B. thoe Schwartzenberg, *Civiel bewijsrecht voor de rechtspraktijk*. Apeldoorn: Maklu 2013.

Szepanski 1979 – W. Szepanski, 'A signal theoretic method for creating forgery-proof documents for automatic verification', in: J. S. Jackson (ed.) Carnahan Con)". *On Crime Countermeasures*, University of Kentucky, Lexington, KY, May 16-18, 1979, pp. 101-109.

Tanaka, Nakamura & Matsui 1990 – K. Tanaka, Y. Nakamura, and K. Matsui, 'Embedding secret information into a dithered multi-level image', *Proceedings of IEEE Military Communications Conference*, Monterey, CA, USA, 1990, pp. 216–220,

Tardos 2003 – G. Tardos, 'Optimal probabilistic fingerprint codes' in: STOC 2003. pp. 116- 125. ACM (2003). Online: http://www.renyi.hu/~tardos/publications.html

Taverne e.a 2013 – M.D. Taverne, M. Malsch, H. Elffers, J.W. de Keijser en P.R. Kranendonk, DNA-rapporten: makkelijker kunnen we het niet maken, begrijpelijker wel. Online: http://www.forensischinstituut.nl/Images/rapport-interpretatie-onderzoeksresultaten_tcm119-492082.PDF

Taylor, Johnson & Crawford 2007 – J. Taylor, M.R. Johnson, C.G. Crawford, *DVD Demystified, Third Edition*, New York: Mc-Graw Hill 2007, pp. 2-7.

Termorshuizen-Arts 2003 (diss.) – M. Termorshuizen-Arts, *Juridische semantiek. Een bijdrage tot de methodologie van de rechts-vergelijking, de rechtsvinding en het juridisch vertalen* (diss. Leiden), Nijmegen: Wolf Legal Publishers 2003.

Telders 1937 – B.M. Telders, Rechtspraak en logica, in: Verzamelde geschriften van prof. mr. B.M. Telders (deel I), 'S-Gravenhage: Martinus Nijhoff 1947, pp. 159-167,

Ten Voorde 2012 – J. Ten Voorde, 'Waarheidsvinding in context. Impressies van de jaarvergadering van de Nederlandse Juristen-vereniging op 8 juni te Rotterdam', NJB 2012, pp. 1856-1861.

Thompson & Schumann 1987 – W. C. Thompson & E.L. Schumann, 'Interpretation of Statistical Evidence in Criminal Trials: The Prosecutor's Fallacy and the Defense Attorney's Fallacy', Law and Human Behavior, Vol 11(3), Sep 1987, pp. 167-187.

Thole e.a. 2010 – E.P.M. Thole, F. van der Jagt, H. Roerdink; 50 vragen over Privacy, Deventer: Kluwer 2010.

Thornbury 1878 – W. Thornbury, 'The Bank of England' in:*Old and New London: Volume 1,* , 1878, pp. 453-473. Online: ttp://www.british-history.ac.uk/report.aspx?compid=45058

Tirkel e.a. 1993 – A.Z. Tirkel, G.A. Rankin, R.M.van Schyndel, W.J. Ho, N.R.A. Mee, C.F. Osborne. 'Electronic Water Mark', *DICTA-93*, Sydney, December 1993, pp. 666-672.

Tjong Tjin Tai 2008– T.F.E. Tjong Tjin Tai, Bewijs van (inhoud van) de overeenkomst, *NJB* 2008, p. 810-816.

TjongTjin Tai & Koops 2015 – E. TjongTjin Tai & B.J. Koops, ‚Zorgplichten tegen cybercrime‘ NJ 2015 90(16), pp. 1065-1072.

Tschundin 2002 – P.F. Tschudin, *Grundzüge der Papiergeschichte*, Stuttgart: Hiersemann, 2002. Online: http://tocs.ub.uni-mainz.de/pdfs/103977112.pdf

Traest 1992 – Ph. Traest, *Het bewijs in strafzaken*, (diss. Gent) Gent: Mys & Breesch, 1992.

Traest 2001 – Ph. Traest, ‘De rol van de particulier in het bewijsrecht in strafzaken: naar een relativering van de uitsluiting van onrechtmatig verkregen bewijs?, in Ý. Poullet en H. Vuye (eds.), *Liber Amicorum Jean du Jardin*, Deurne: Kluwer, 2001, pp. 61-78.

Traest 2004 – Ph. Traest, ‘Onrechtmatig verkregen doch bruikbaar bewijs: het Hof van Cassatie zet de bakens uit’, *T.Strafr.* 2004, annotatie onder Cass. 14 oktober 2003.

Tijssen 2009 (diss.) – H.E.B. Tijssen, *De juridische dissertatie onder de loep. De verantwoording van methodologische keuzes in juridische dissertaties* (diss. Tilburg), Den Haag: BJU 2009. Online: http://arno.uvt.nl/show.cgi?fid=94878

TNO 2010 – TNO, Privacytoets HDIeF (Herkenning Digitale Informatie en Fingerprinting) (NCTb), 2011-12, 31 maart 2010. Online: nctv.nl/Images/prnu-deel-2_tcm126-444147.pdf

Toom 2009 – V. Toom, ‘De wereld achter het DNA-bewijs: betrouwbaarheid in een Nederlands laboratorium voor DNA-onderzoek’, NJB 2009/328, pp. 416-423.

Toom 2010 (diss.) – V. Toom, *Dragers van waarheid. Normatieve aspecten van twintig jaar forensisch DNA-onderzoek in Nederland* (diss. UvA), Amsterdam: Universiteit van Amsterdam 2010. Later ook uitgegeven door Kluwer, 2011. Online: http://dare.uva.nl/document/187415

Toussaint 2005 – P. Toussaint, ‘La loi des juges’, Journ. proc. 2005, nr. 499, p. 31. Annotatie onder Cass. 2 maart 2005).

Tversky & Kahneman 1974 – A. Tversky & D. Kahneman, ‘Judgment under Uncertainty: Heuristics and Biases’ *Science, New Series*, Vol. 185, No. 4157. (Sep. 27, 1974), pp. 1124-1131.

Twining 1994 – W. Twining, *Rethinking evidence: Exploratory Essays*, Illinois: Northwestern Univerity Press, 1994.

Twining 2003 – W. Twining, ‘Evidence as a multi-disciplinary subject’, Law, Probability and Risk 2003, p. 91-107.

’t Hart 2001 - A. C. ’t Hart, ‘De autonomie van het strafrecht’, *DD* 2001,31, pp. 237-250

Ubbink 1966 – J.B. Ubbink, ‘Het bewijs in de natuurwetenschap’, Rechtsgeleerd Magazijn Themis, 1966, pp. 432 – 460.

Van Asperen de Boer 2007 – C.M.I van Asperen de Boer, *De rol van statistiek bij strafrechtelijke bewijsvoering, in het bijzonder in dienstroosterzaken*, Gelling Publishing, 2007.

Van Boom, Giesen en Verheij 2013 – W.H. Van Boom, I. Giesen en A.J. Verheij, *Capita Civilogie, Handboek empirie en recht*, Den Haag: BJU 2013, tweede druk.

Van Compernolle 2002 – J. van Compernolle, ‘Le rôle du jugedans la cîté: versungouvernement des juges!’, in: Le rôle du jugedans la cîté, Brussel: Bruylant 2002.

Van Compernolle 2011 – J. van Compernolle ‘L’incidence de la jurisprudence de la Cour européenne des droits de l’homme sur l’administration de la preuve dans le procès civil’ in G. *De Leval (ed.), La preuve et la diffi cile quête de la vérité judiciaire*, Anthemis:Luik, 2011, (7), p. 14-15.

Van Daalen 2002 – O. van Daalen, ‘Hollywood verliest controle over digitale distributie’, *I&I* 2002-5, p. 8-15.

Van Damme 2009 – K. van Damme, *Het auteursrecht in de boekensector*, Die Keure 2009.

Van Doninck 2011 – J. Van Doninck, *Onrechtmatig bewijs in civiele zaken.: willen we de waarheid?*, Openingsrede van 24 november 2011 ter gelegenheid van de plechtige openingszitting van het 121e werkingsjaar van het Vlaams Pleitgenootschap bij de Balie te Brussel, Antwerpen, Intersentia, 2011.

Van Dort 2000 – R.M.J.T. van Dort, ‘Privacy-onderzoek in de letselpraktijk: Slachtoffer of verdachte?’, *Het Verzekerings-Archief* 2000 1/2, p. 5-11.

Van Duyne & Kwanten 2004 – P.C. van Duyne van en C.H.N. Kwanten, (2004), *Handhaven: eerst kiezen, dan doen. Juridische grenzen en mogelijkheden* (deelrapport V), Den Haag: Ministerie van Justitie.

Van den Brink 2008 – V. van den Brink, 'Stellen, betwisten, bewijzen – een handleiding', PP 2008, pp. 989-100.

Van den Eshof e.a. 2002 – G.L.M. van den Eshof, P.H.M. Spronck, G.W. Boers, J.P.G.M.Verbeek & H.J. van den Herik, *Opsporing van verborgen informatie: Technische mogelijkheden en juridische beperkingen,* ITeR-reeks 56, Den Haag: Sdu Uitgevers 2002. Online: http://ejure.nl/downloads/dossier_id=228/id=90/show.html

Van der Leun 2013 – J.P. van der Leun, 'Zal de strafbaarstelling van illegaliteit effectief zijn? En wil iemand dat eigenlijk weten?, AA 2013/1, pp. 8-18 (AA20130008).

Van der Pol 2006 – R.A. van der Pol, 'Het aanbod van getuigenbewijs', *TCR* 2006-2, pp. 35-38.

Van Engelen 1994 – Th. C.J.A. van Engelen, *Prestatiebescherming en ongeschreven intellectuele* eigendoms-rechten, Zwolle: W.E.J. Tjeenk Willink 1994 (diss. Leiden).

Van Esch 2007 – R.E. van Esch, *Juridische aspecten van elektronische handel*, Deventer: Kluwer 2007, p. 125.

Van Gerven 1995 – W. van Gerven, 'Het proportionaliteitsbeginsel', in: De norm achter de regel (Storme-bundel), Deurne: Story-Scientia, 1995, pp. 3-17.

Van Gerven 2006 – W. van Gerven, m.m.v. S. Covemaeker, *Verbintenissenrecht*, Leuven: Acco 2006

Van Gestel & Vranken 2007 – R.A.J. van Gestel en J.B.M. Vranken, 'Rechtswetenschappelijke artikelen; Naar criteria voor methodologische verantwoording, *NJB* 2007-24, pp. 1448-1461.

Van Grinten 1960 – W.C.L. van der Grinten, Ars Aequi X, oktober 1960.

Van Kildonck 2010 – K. van Kildonck, Privacy werknemers. Onrechtmatig verkregen bewijs op het werk, *NjW*, nr. 218, pp. 180-183.

Van Koppen 2005 – P.J. van Koppen, *Paradoxen van deskundigen. Over de rol van experts in strafzaken*. (Oratie Maastricht), Deventer: Kluwer, 2004.

Van Koppen 2005 – P.J. van Koppen, 'Het experiment in de rechtspsychologie', *Tijdschrift voor Criminologie*, pp. 413-418.

Van Koppen 2011 – P.J. van Koppen, *Overtuigend bewijs: Indammen van rechterlijke dwalingen*. Amsterdam: Nieuw Amsterdam, 2011.

Van Lambalgen & Meester 2004 - M. van Lambalgen en R.W.J. Meester (2004), 'Wat zeggen al die getallen eigenlijk ? De statistiek in het proces tegen Lucia de B.', Trema, 2007/7, p. 286-292. Online: http://staff.science.uva.nl/~michiell/docs/LuciadeB040205.pdf

Van Ommeslaghe 2004 – P. van Ommeslaghe, 'La preuve des obligations et de celle de leur paiement, *JT* 2004, p. 300-302.

Van Soeren 1986 – W.H. van Soeren, 'Onrechtmatig verkregen bewijs in de civiele procedure', AA 1986, pp. 483-489.

Van Stekelenburg 2009 (diss.) – M.C. Van Stekelenburg - *De betere byte in de strijd om het gelijk. Een onderzoek naar de betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht* (diss. Amsterdam VU), Delft: Eburon 2009.

Van Vlooten 2011 – R. Van Vlooten, **'**Implementatie van artikel 14 Handhavingsrichtlijn: lost in translation?'in: Van Boom, Van Dam-Lely en Lindenbergh (red.), *Rake remedies. Opstellen over handhaving van rechten, naleving van plichten en sanctionering van verkeerd gedrag in het privaatrecht*, Den Haag, BJu 2011, p. 231-255.

Van Volsem 2008 – F. van Volsem, 'Antigoon: geen spook maar een reddende engel bij de foutieve uitvoering van een correct bevolen tapmaatregel', *RABG* 2008/7, pp. 440-447. Annotatie onder Cass. 19 juni 2007.

Van Zwet 2004 – W. van Zwet, 'Niets nieuws onder de zon', STAtOR 5/2, p. 21-29.

Verbruggen 2006 – F. Verbruggen, 'Vindt het spook van Antigoon rust? Franstalig 'schoonmoedersarrest' als slotluik van de nieuwe cassatierechtspraak over de uitsluiting van onrechtmatig bewijs', T. Strafr. 2006, 25, annotatie onder Cass 12 oktober 2005.

Verhelst & Thoelen 2008 – I. Verhelst en N. Thoelen, 'Over privacy, controle en (on)rechtmatig verkregen bewijs', *Or.* 2008, pp. 197-208.

Verkerk 2007 – R.R. Verkerk, 'Procesrechtelijke waarborgen voor een betrouwbaar deskundigenonderzoek', *NTBR* 2007, 71, pp. 491-500.

Verkerk 2010 (diss.) – R.R. Verkerk, *Fact-finding in civil litigation, a comparative perspective* (diss. *Maastricht*), Antwerp: Intersentia, 2010.

Verstraeten & De Decker 2005 – R. Verstraeten en S. De Decker 'Antigoon sluit de achterpoort, maar opent een raam', *T. Strafr.* 2005, 285, annotatie onder Cass. 16 november 2004.

Verstraeten 2005 – R. Verstraeten, Handboek strafvordering, 5e druk, Antwerpen/Apeldoorn: Maklu 2005

Verstraeten 2012 – R. Verstraeten, *Handboek strafvordering*, 5e druk, Antwerpen/Apeldoorn: Maklu 2012

Visser 2004 – D.J.G. Visser, *Het ABC van iedere IE-inbreuk, Het belang van de rest van de markt*, Boom Juridische uitgevers, Den Haag 2004.

Visser 2008 – D.J.G. Visser, 'Beslissen in IE zaken'. *NJB* 2008-31, pp. 1918-1926.

Visser 2009 – D.J.G. Visser, 'De rechterlijke beslissing (in IE-zaken)', (www.ie-forum.nl) *IEF* 8189, 2009.

Visser 2010 – D.J.G. Visser, Het 'embedden' van een You Tube-filmpje op een Hyves-pagina, *Mf* 2010/1, pp. 12-16.

Visser & De Jager 2010 – Dirk Visser & Gerrit de Jager, *Te intellectuele eigendom, De morele basisemoties van de IE*, deLex 2010.

Visser 2011a – D.J.G. Visser, *Motiveren in IE-zaken, een handleidig voor het motiveren van een beslissing in een eenvoudige IE-zaak*, deLex 2011.

Visser 2011b, – D.J.G. Visser, 'Repliceren in IE-zaken, *BIE* 2011, pp. 320-325.

Voulon 2010 – M.B. Voulon, *Automatisch contracteren* (diss Leiden), Leiden University Press 2010

Voulon 2013 – M.B. Voulon, 'Een Europese verordening voor identity management (IdM)', CR 2013/118, pp. 196-204.

Voulon 2014 – M.B. Voulon, 'Bewijs en bewaren', in: S. van der Hof, A.R. Lodder & G.J. Zwenne (red.), *Recht en Computer*, Deventer: Kluwer, 2014.

Voyatzis, Nikolaides & Pitas 1998 - G. Voyatzis, N. Nikolaides & I. Pitas, 'Digital watermarking: An overview', in: *Proceedings IX European Signal Processing Conference* (EUSIPCO), Island of Rhodes, Greece, Sept. 8-11, 1998, p. 13-16. Online: http://www.wizpia.com/files/paper/12-02-2001/voyatzis98digital.pdf

Voyatzis & Pitas 1999 – G. Voyatzis, I. Pitas, 'Protecting Digital Image Copyrights: A Framework', *IEEE*, Volume 19 Issue 1, January 1999, pp. 18-24.

Vranken 2000 – J.B.M. Vranken, 'Onrechtmatig verkregen bewijs in civiele zaken. Bespreking van het gelijknamige proefschrift van M. Kremers', TCR 2000, pp. 59-61.

Vranken & Van Gestel 2010 – J.B.M. Vranken & R.A.J. van Gestel, 'Vertrouwen is goed, controle niet altijd beter', *AA* maart 2010, pp. 166-179.

Vranken 2014 - J.B.M. Vranken, Algemeen deel**** (Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht) , Deventer: Kluwer 2014

Vrendenbarg 2013 – C.J.S. Vrendenbarg: 'De 'volledige' proceskostenveroordeling in IE-zaken. Een kritische bespreking van de implementatie en interpretatie van artikel 14 Handhavingsrichtlijn in Nederland', *BIE* 2013, pp. 160-169.

Wagner 2008 – K. Wagner, 'Recente ontwikkelingen met betrekking tot het bewijs in burgerlijke zaken', in D. Serrrus (ed.), *Actualia gerechtelijk recht*, studiecyclus Vlaamse Conferentie van de Balie te Gent, Brussel, Larcier, 2008, pp. 141-

Wagner 2009 – K. Wagner 'Actualia burgerlijk bewijsrecht', *P&B / RDJP* 2009, p. 153-172.

Wang, Doherty & Dyck 2002 - Y. Wang, J.F. Doherty & R.E.V. Dyck, 'A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images', IEEE Transactions on Image Processing, vol. 11, nr. 2, 2002, pp. 77-88.

Weda e.a. 2011 - J. Weda, I. Akker, J. Poort, P. Rutten en A. Beunen, Wat er speelt. De positie van makers en uitvoerend kunstenaars in de digitale omgeving. Amsterdam, maart 2011. Online: http://wodc.nl/onderzoeksdatabase/de-positie-van-individuele-makers-en-uitvoerende-kunstenaars.aspx?cp=44&cs=6802

Wendell Holmes 1897 – O. Wendell Holmes, Jr., 'The Path of the Law', vol. 10 *Harvard Law Review* (1897).

Werkers e.a. 2009 – E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, 'Auteursrecht in de digitale samenleving', Studie in opdracht van de Vlaamse Gemeenschap Departement Cultuur, Jeugd, Sport en Media, Leuven, 2009. Online: http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

Westerman & Wissink – P. Westerman & M. Wissink, 'Rechtsgeleerdheid als rechtswetenschap', *NJB* 2008-2009.

Wetzels 2011 – W.J.J. Wetzels, 'De kantonrechter en/of de civiele rechter van de toekomst', *TvPP* 2011-1, pp. 19-20.

Wiersma 2010 – H.M. Wiersma, 'Bewijswaarderingsoordelen in het civiele (proces)recht', *AA* 2010, pp. 466-475.

Wigmore 1931 – J.H. Wigmore, *The Principles of Judicial Proof or the Process of Proof as Given by Logic, Psychology, and General Experience, and Illustrated in Judicial Trials*, 2nd edition, Little, Brown and Company, Boston (Massachusetts), 1931.

Wistrich, Guthrie, & Rachlinski 2005 – A.J. Wistrich, C. Guthrie, J.J. Rachlinski, 'Can Judges Ignore Inadmissible Information: The Difficulty of Deliberately Disregarding', University of Pennsylvania Law Review 2005, 153(4), pp. 1253-1345.

WODC 2005 – WODC, *Forensisch DNA-onderzoek: een rechtsvergelijkende verkenning. Rapportage van een rechtsvergelijkend onderzoek naar de regelgeving en de praktijk van het forensisch DNA-onderzoek in Nederland, België, Duitsland, Engeland & Wales en Frankrijk*., 2005. Dit onderzoek is uitgevoerd in opdracht van het WODC door C. van den Heuvel, J.F. Nijboer, A.M. van Rijsewijk, en Th. A. de Roos.

Wolters Ruckert 2012 – N. Wolters Ruckert, 'Het begrip "persoonsgegeven", een schaap in wolfskleren?', *Mf* 2012-1, p. 1.

Zhao 1996 – J. Zhao, 'A WWW service to embed and prove digital copyright watermarks' in:
European Conference on Multimedia Applications, Services and Techniques, Louvain-la-Neuve, Belgium, May 1996, pp. 695-710.

Zhao, Koch & Luo 1998 – J. Zhao, E. Koch, C. Luo, 'In Business Today and Tomorrow', Communication ACM 41(7) 1998: pp. 66-72.

Zhu & Liu 2009 – S. Zhu, J. Liu, 'A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization', Lecture Notes in Computer Science, Vol. 5451, 2009, pp. 136-146

Zweigert & Kotz 1998 – K. Zweigert & H. Kötz, *Introduction to Comparative Law*, 3e druk Oxford 1998.

Jurisprudentieregister

Europa

Europees Hof voor de Rechten van de Mens (ERHM)

EHRM 23 november 1993, nr. 14838/89 (A/Frankrijk);
EHRM 12 juli 1988, NJ 1988, 851 (Schenk);
EHRM 8 februari 1996, NJ 1996, 725 (Murray);
EHRM 18 maart 1997, NJ 1998, 278, m.nt. Snijders (Mantovanelli/Frankrijk);
EHRM 9 juni 1998, NJ 2001, 471, m.nt. Kn (Texeira de Castro);
EHRM 27 juni 2001, NJ 2002, 102 (Rodriguez);
EHRM 12 mei 2000, NJCM Bulletin, p. 1255, m.nt. E. Myjer (Kahn/Verenigd Koninkrijk);
EHRM 8 april 2003, NbSr 2003, 185 (M.M./Nederland);
EHRM 3 april 2007, RDTI 2007, (371) 371, m.nt. NJ 2007-50, 617, pp. 6232-6236, m.nt. EJD (Copland/Verenigd Koninkrijk);
EHRM 28 juli 2009, ECLI:NL:XX:2009:BK4631 RABG, 2010/1, m.nt. F. Schuermans; NJ, 2010, 627. m.nt. YB; RDPC 2010, 312, m.nt. N. Colette-Basecqz RW 2011-12, 24, m.nt. A. Verduyckt (Lee Davies/België);
EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, NJB 2011, 236, NJ 2011/566 m.nt. EJD (Köpke/Duitsland).

Europees Hof van Justitie van de Europese Unie (HvJ EU)

HvJ EG 29 januari 2008, zaak C-275/06, Jur. p. I-271, AMI 2008/5, p. 67, m.nt. Ekker; IER 2008/44, p. 158, m.nt. FWG, CR 2008/94 m.nt. Rob van Esch (Promusicae/Telefónica);
HvJ EG 16 juli 2009, 16 juli 2009, zaak C-5/08, Jur. p. I-6569, NJ 2011, 288, m.nt. PBH (Infopaq);
HvJ EU 30 september 2010, zaak C-581/08, ECLI:EU:C:2010:559, NTFR 2010, 2319 m.nt. Sanders (EMI Group)
HvJ EU 21 oktober 2010, zaak C-467-08, m.nt. PBH, NJ 2011-47/510, p. 5217-5219 (Padawan/SGAE) ;
HvJ EU 22 december 2010, zaak C-393/09, NJ 2011, 289, m.nt. PBH (BSA);
HvJ EU 4 oktober 2011, zaken C-403/08 en C-429/08, ov. 154 en 185 (Premier League);
HvJ EG 24 november 2011, zaak C-70/10, AMI 2011/2, m.nt. EJD, Mf 2012/3, m.nt. Kulk & Borgesius (Scarlet/Sabam);
HvJ EU 1 december 2011, zaak C-145/10, IER 2012/16, p. 143-162, NJ 2013-7, 66, p. 761-778,m.nt. De Boer en Hugenholtz (Eva Maria Painer);
HvJ EU 16 februari 2012, zaak C-360/10 (SABAM tegen Netlog), NJ 2012, 479 en 480, p. 5395-5397,m.nt.PBH
HvJ EU 26 april 2012, zaak C-510/10 (DR en TV2 Danmark/NCB);
HvJ EU 19 april 2012, zaak C-461/10 (Bonnier Audio);
HvJEU 3 juli 2012, zaak C-128/11, UsedSoft/Oracle, NJ 2013, 118, mnt. PBH, AMI 2013/3 (met commentaren van MRF, p. 76, M. Senftleben op p. 56 en FWG op p. 61);
HvJ EU 23 januari 2014, zaak C-352/12, AMI 2014/2 m.nt. Koelman (Nintendo/PC Box);
HvJ EU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien);
HvJ EU 10 april 2014, zaak C-435/12 (ACI Adam/Stichting De Thuiskopie).

NEDERLAND

Hoge Raad der Nederlanden

HR 8 juni 1931, NJ 1932, p. 1550;
HR 19 december 1949, NJ 1950, 51;
HR 9 november 1954, NJ 1955, 55, m.nt. WP. (Cicero);

HR 29 november 1957 NJ 1958, 31, NJ 1958/31, BIE 1958, p. 45, AA 1957/58, p. 145 m.nt. DM;
HR 8 januari 1965, NJ 1965, 162 (ETBI/Behangselpapierfabrieken);
HR 4 juni 1976, NJ 1988, 417;
HR 31 januari 1975, ECLI:NL:HR:1975:AC5538;
HR 12 december 1978, NJ 1979, 142;
HR 7 maart 1980, NJ 1980/365;
HR 15 september 1980, NJ 1981, 13;
HR 10 december 1982, NJ 1983, 687, m.nt. EAA (Binderen/Kaya);
HR 1 juni 1984, NJ 1984, 630, m.nt. WHH (Peeters/Van Raaij);
HR 19 februari 1985, NJ 1985, 633 (Cocaïne in koffer);
HR 16 december 1986, NJ 1987, 613 (Verhuur illegale kopieën);
HR 9 januari 1987, NJ 1987/928, m.nt. E.A. Alkema: AB 1987/231, m.nt. F.H. van den Burg; CR 1987, p. 110, m.nt. E.J. Dommering; NJCM-bulletin 1987, p. 298, m.nt. L. Verhey en Nemesis 1986, p. 274.; zie voorts A. van Baalen, NJB 1987, p. 754; B.F. de Jong, NJB 1987, p. 758 en G. Overkleeft/Verburg, AA 1988/27, p. 1110 (Edamse bijstandsmoeder);
HR 16 oktober 1987, ECLI:NL:HR:1987:AC9997, NJ 1988, 850, m.nt EAA (Driessen/Van Gelder);
HR 13 december 1988, ECLI:NL:HR:1988:AC3339, NJ 1989, 499 (Verveelvoudiging van studieboeken);
HR 12 mei 1989, NJ 1989, 596 (Dolmans/Wouters);
HR 7 februari 1992, ECLI:NL:HR:1992:ZC0500, NJ 1993/78 m.nt. H.J. Snijders (Slempkes/Nool);
HR 21 februari 1992, AMI 1993, p. 7, m.nt. Gerbrandy; IER 1992, p. 89, m.nt AAQ; NJ 1993, 164, m.nt. JHS; 2000, 309; BIE 1993, 65, p. 246 (Cindy/Barbie);
HR 8 juli 1992, NJ 1992, 713;
HR 9 oktober 1992, NJ 1994/535, m.nt. CJHB;
HR 22 januari 1993, NJ 1993, 665;
HR 12 februari 1993, ECLI:NL:HR:1993:AJ8237, NJ 1993/599 m.nt. H.J. Snijders & E.A. Alkema (W./gemeente Spijkenisse);
HR 18 mei 1993, NJ 1993, 728;
HR 25 juni 1993, NJ 1993/686, m.nt. PAS;
HR 10 september 1993, NJ 1994, 272;
HR 19 november 1993, NJ 1994, 622, m.nt. JCS (COVA);
HR 18 februari 1994, NJ 1994, 368;
HR 13 januari 1995, ECLI:NL:HR:1995:ZC1611, NJ 1997, 175, m.nt. CJHB;
HR 11 april 1995, ECLI:NL:HR:1995:ZC9998, NJ 1995, 537 m.nt. Corstens;
HR 15 december 1995, NJ 1996, 509 (Procter & Gamble/Kimberley-Clark);
HR12 maart 1996, NJ 1996, 539;
HR 7 mei 1996, NJ 1996, 573;
HR 10 januari 1997, NJ 1999, 286 m.nt. WMK;
HR 13 mei 1997, NJ 1997, 152;
HR 27 januari 1998, NJ 1998, 404 (Schoenmakersarrest);
HR 16 oktober 1998, NJ 1999, 7;
HR 6 april 1999, NJ 1999, 566 (Octopuszaak II);
HR 16 april 1999, ECLI:NL:HR:1999:ZC2887, NJ 1999, 666, m.nt. P. Clausing;
HR 1 juni 1999, AA 49, 2000, p. 117-121 m. nt. YB;
HR 21 november 2000, ECLI:NL:HR:2000:AA8408;
HR 27 april 2001, ECLI:NL:HR:2001:AB1347, NJ 2001/421, m.nt. PAS (L/Wennekes Lederwaren);
HR 8 mei 2001, ECLI:NL:HR:2001:AB1517, NJ 2001 479;
HR 26 juni 2001, ECLI:NL:PHR:2001:AA9800, NJ 2001, 564, m.nt. Sch. (Herziening Puttense moordzaak II);
HR 29 juni 2001, NJ 2001, 495;
HR 7 september 2001, NJ 2001, 615;
HR 23 november 2001, NJ 2002, 387;

HR 30 november 2001, ECLI:NL:HR:2001:AD4000 NJ 2002, 462 m.nt. JdB;
HR 8 januari 2002, ECLI:NL:HR:2002:AD5594, NJ 2002, 340 m.nt. Sch;
HR 12 februari 2002, ECLI:NL:HR:2002:AD5201, NJ 2002/330;
HR 31 mei 2002, ECLI:NL:HR:2002:AD9609, NJ 2003, 589, m.nt. JBMV; JBPR 2002/2 m.nt. W.C.G.M. van Hoof en J.G.A. Linssen;
HR 1 november 2002, NJ 2005, 281;
HR 6 december 2002, NJ 2003, 63 (Goedèl/Arts);
HR 10 december 2002, ECLI:NL:HR:2002:AE6863;
HR 14 januari 2003, ECLI:NL:HR:2013:AE9038, NJ 2003, 288, .m.nt. YB;
HR 18 maart 2003, ECLI:NL:HR:2003:AF4321, NJ 2003, 527;
HR 2 mei 2003, NJ 2003, 468;
HR 5 december 2003, ECLI:NL:HR:2003:AN8478, JBPR 2004/29 m.nt. Schellaars (Nieuw Vredenburgh/Nieuwe Hollandse Lloyd);
HR 30 maart 2004, ECLI:NL:HR:2004:AM2533, NJ 2004, 376 m.nt. Buruma;
HR 7 mei 2004, ECLI:NL:HR:2004:AO2988, NJ 2004, 422 m.nt. DA;
HR 19 november 2004, ECLI:NL:PHR:2004:AR5917;
HR 25 januari 2005 ECLI:NL:PHR:2005:AS1872 (Herziening Schiedammer Parkmoord II);
HR 25 maart 2005, ECLI:NL:HR:2005:AT0412, JPF 2005/56 m.nt. P. Vlaardingerbroek (vaststellen vaderschap);
HR 8 november 2005, ECLI:NL:HR:2005:AU3292, NJ 2006/136;
HR 25 november 2005, ECLI:NL:HR:2005:AU4019, CR 2006, 11 m.nt. H.H., IER 2006, 2 m.nt. JK, NJ 2009, 550 m.nt. PBH (Lycos/Pessers);
HR 20 januari 2006, NJ 2006, 78, JBPr 2006, 44 m. nt. Rueb;
HR 24 februari 2006, NJ 2007, 37 (Technip/Goossens);
HR 14 maart 2006, ECLI:NL:HR:2006:AU5496, NJ 2007, 345, m.nt. P.A.M. Mevis (Lucia de B.);
HR 9 juni 2006, NJ 2006, 327;
HR 5 september 2006 ECLI:NL:HR:2006:AV4122;
HR 31 oktober 2006, ECLI:NL:PHR:2006:AX9179
HR 14 november 2006, ECLI:NL:HR:2006:AX7471, NJ 2007, 179, m.n. YB (KB-Lux)
HR 17 november 2006, NJ 2006, 621;
HR 15 december 2006, ECLI:NL:HR:2006:AZ1083, NJ 2007/ 203, m.nt. Mok (NNE/Mourik);
HR 20 februari 2007, NJ 2007, 313 m.nt. Buruma (HIV-III);
HR 1 juni 2007, ECLI:NL:HR:2007:BA3525;
HR 15 juni 2007, ECLI:NL:HR:2007:BA3587, NJ 2007, 335;
HR 2 oktober 2007, ECLI:NL:HR:2007:BA5831, NJ 2007, 545;
HR 30 oktober 2007, ECLI:NL:HR:2007:BA6569;
HR 22 februari 2008, ECLI:NL:HR:2008:BB5626, JA 2008/72 m.nt. J. Quakkelaar;
HR 30 mei 2008, ECLI:NL:HR:2008:BC2153, NJ 2008, 556 (Endstra/Nieuw Amsterdam; De Endstra Tapes);
HR 11 juli 2008, ECLI:NL:HR:2008:BC8421, NJ 2009, 451 m.nt. Dommering (De Telegraaf);
HR 30 september 2008, ECLI:NL:HR:2008:BD4872;
HR 7 oktober 2008, ECLI:NL:HR:2008:BD4153, NJ 2009, 44 m. nt. P.A.M. Mevis (herziening Lucia de B.);
HR 16 januari 2009, ECLI:NL:HR:2009:BG4012, NJ 2009, 562 m.nt. Snijders;
HR 17 april 2009 ECLI:NL:PHR:2009:BH2955, NJ 2009, 196;
HR 20 november 2009, ECLI:NL:HR:2009:BJ6999, BIE 2010, 4, m.nt. PJMS, IER 2010, 16 m.nt. FWG, NJ 2011/302 m.nt. JHS (Lego/Mega Brands);
HR 8 december 2009, ECLI:NL:HR:2009:BI5746;
HR 15 december 2009, ECLI:NL:HR:2009:BK2129 NJ 2010, 26;
HR 2 februari 2010, ECLI:NL:HR:2010:BJ7266;
HR 2 november 2010, ECLI:NL:HR:2010: BN6801;

HR 4 januari 2011, ECLI:NL:HR:2011:BM6673, VA 2012/6, m.nt. M.L.C.C. de Bruijn-Lückers NJ 2012/145 m.nt. M.J. Borgers;
HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251, NJ 2012, 536 m. nt. N. Keijzer, IR 2012, p. 50 T. Peijnenburg (Runescape);
HR 20 maart 2012, ECLI:NL:HR:2012:BV7501;
HR 10 april 2012, ECLI:NL:HR:2012:BU7636, NJ 2012/264;
HR 18 januari 2013, ECLI:NL:HR:2013:BY0535;
HR 13 september 2013, ECLI:NL:HR:2013:BZ9958, IER 2014/9, m.nt. F.W.E. Eijsvogels, JOR 2013/330, m.nt. E. Loesberg (Molenbeek Invest/Begeer c.s.);
HR 25 oktober 2013, ECLI:NL:HR:2013:1036, AMI 2014/6, m.nt. M.R.F. Senftleben (p. 41-46), IER 2014/6 m.nt. PGFAG; BIE 2014/38 (S&S/Esschert; Vuurkorven);
HR 4 april 2014, ECLI:NL:HR:2014:831, JA 2014/78 m.nt J. Veninga & F.T. Oldenhuis NJ 2014/368 m.nt. T. Hartlief, AB 2014/228 m.nt. A. Hofman
HR 18 april 2014, ECLI:NL:HR:2014:942, *JA* 2014/65 m.nt. M.H.J. Lubbers & P. Oskam, *JIN* 2014/113 m.nt. R.D. Leen, NJ 2015/20 met annotatie door M.M. Mendel en H.B. Krans (Achmea/Rijnberg);
HR 11 juli 2014, ECLI:NL:HR:2014:1632 *JIN* 2014/175 m.nt. P.C.M. Kemp, *JBPr* 2014/52 m.nt. M. Kremer;
HR 11 november 2014 ECLI:NL:HR:2014:3142, JIN 2014/228 m.nt. C.J.A. de Bruijn.

Hoven

Hof Amsterdam 14 mei 1929, NJ 1930 1616;
Hof ’s-Hertogenbosch 2 juli 1986, ECLI:NL:GHSHE:1986:AC9463 (Koma);
Hof Amsterdam 26 april 2001, ECLI:NL:GHAMS:2001:AD4264;
Hof Leeuwarden 24 april 2002, ECLI:NL:GHLEE:2002:AE1877 (Vrijspraak Puttense Moordzaak);
Hof Amsterdam 7 oktober 2003 ECLI:NL:GHAMS:2003:AL7736;
Hof ’s-Gravenhage 18 juni 2004, ECLI:NL:GHSGR:2004:AP2846 (Lucia de B.);
Hof Amsterdam 24 juni 2004, rolnr. 1689/03KG;
Hof ’s-Hertogenbosch 8 juni 2004, ECLI:NL:GHSHE:2004:AP2368 , AMI, nr, 14 (Lancôme / Kecofa);
Hof ’s-Hertogenbosch 27 september 2004, ECLI:NL:GHSHE:2004:BQ1759;
Hof Amsterdam 4 mei 2006, ECLI:NL:GHAMS:2006:AW8270 (Schiedammer Parkmoord);
Hof Amsterdam 13 juli 2006, ECLI:NL:GHAMS:2006:AY3854, CR 2006, 168 m. nt. N.M. Wisman (Brein/Kazaa);
Hof Amsterdam 13 juli 2006, ECLI:NL:GHAMS:2006:AY3864 (Lucia de B.);
Hof ’s-Hertogenbosch 25 januari 2007, ECLI:NL:GHSHE:2007:AZ8027;
Hof ’s-Hertogenbosch 8 juni 2004, ECLI:NL:GHSHE:2004:AP2368 , AMI 2004/14, m.nt. JHS (Lancôme / Kecofa);
Hof ‘s-Gravenhage 16 april 2008, ECLI:NL:GHSGR:2008:BM1620, NJ 2010, 204
Hof Arnhem 3 maart 2009, ECLI:NL:GHARN:2009:BI1243;
Hof Amsterdam 16 maart 2010, ECLI:NL:GHAMS:2010:BL7920, IER 2010, 78 m.nt. MdCB (e-Donkey);
Hof ’s-Gravenhage 23 maart 2010, ECLI:NL:GHSGR:2010:BM1155;
Hof Arnhem 14 april 2010, ECLI:NL:GHARN:2010:BM0876, NJ 2010, 363 m.nt. P.A.M. Mevis (Vrijspraak Lucia de B.);
Hof Leeuwarden 4 mei 2010, ECLI:NL:GHSGR:2010:BO8246;
Hof ’s-Gravenhage 29 juni 2010, ECLI:NL:GHSGR:2010:BN8145;
Hof ’s-Gravenhage 22 oktober 2010, ECLI:NL:GHLEE:2010:BM3169;
Hof ’s Gravenhage, 15 november 2010, ECLI:NL:GHSGR:2010:BO3980, IER 2011, 28 m. nt. K.J. Koelman, NJ 2011, 565 (FTD/Eyeworks);
Hof Amsterdam, 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (Ziggo/123 Video);
Hof ‘s-Gravenhage 22 december 2010, ECLI:NL:GHSGR:2010: BO8237, BO8239, BO8240, BO8243, BO8245, BO8246, BO8248, m.nt. Duker, AMI 2011/5, nr. 9, (e-donkey);
Hof ’s-Hertogenbosch 30 maart 2011, ECLI:NL:GHSHE:2011:BP9521;

Hof Leeuwarden 5 december 2011, ECLI:NL:GHLEE:2011:BU6824;
Hof ’s-Hertogenbosch 4 september 2012, ECLI:NL:GHSHE:2012:BX9465 (Achmea/Rijnberg);
Hof Den Haag 18 januari 2013, ECLI:NL:GHDHA:2013:BZ6496, CR 2013/161 m.nt. J.J. Oerlemans;
Hof Den Haag 30 september 2013, ECLI:NL:GHDHA:2013:3706;
Hof Den Haag 29 oktober 2013, ECLI:NL:GHDHA:2013:3941;
Hof Den Haag 27 januari 2014, ECLI:NL:GHDHA:2014:84 (5.000 e-books);
Hof Amsterdam, 20 januari 2015 ECLI:NL:GHAMS:2015:66 (NUV/Tom Kabinet).

Rechtbanken

Rb. ‘Hertogenbosch 24 maart 1941, NJ 1941, 783;
Rb. ‘s-Gravenhage 24 maart 2003, ECLI:NL:RBSGR:2003:AF6172 (Lucia de B.);
Rb. Arnhem 3 maart 2005, ECLI:NL:RBARN:2005:AS8529;
Rb. Haarlem 24 mei 2006, JAR 2006/197;
Rb. ‘s-Gravenhage 31 juli 2006, ECLI:NL:RBSGR:2006:AY5348;
Rb. Breda 25 oktober 2006, ECLI:NL:RBBRE:2006:AZ1374;
Rb. Rotterdam 24 juli 2007, ECLI:NL:RBROT:2007:BB0268 (E-donkey);
Rb. Rotterdam 6 augustus 2008, ECLI:NL:RBROT:2008:BD9713;
Rb. Amsterdam 11 september 2008, ECLI:NL:RBAMS:2008:BF0824 (Bandbreedte);
Rb. ’s-Hertogenbosch 2 oktober 2008, ECLI:NL:RBSHE:2008:BF9979;
Rb. ’s-Hertogenbosch 29 oktober 2008, ECLI:NL:RBSHE:2008:BG3640;
Rb. Haarlem 19 november 2008, ECLI:NL:RBHAA:2008:BG5139;
Rb. Utrecht 1 december 2008, ECLI:NL:RBUTR:2008:BG5730;
Rb. ’s-Gravenhage 4 december 2008, ECLI:NL:RBSGR:2008:BG6090;
Rb. ’s-Hertogenbosch 24 december 2008, ECLI:NL:RBSHE:2008:BG9125;
Rb. Leeuwarden 9 april 2009, ECLI:NL:RBLEE:2009:BI0666;
Rb. Amsterdam 3 juli 2009 ECLI:NL:RBAMS:2009:BJ8160;
Rb. Arnhem, 9 september 2009, ECLI:NL:RBARN:2009:BJ8844 (Coca-Cola/ Superunie);
Rb. ’s-Gravenhage, 25 november 2009, IER 2010, 10 (G-Star/Pepsi Raw II);
Rb. Amsterdam 26 november 2009, ECLI:NL:RBAMS:2009:BK7336;
Rb. Middelburg 2 december 2009, ECLI:NL:RBMID:2009:BL9868;
Rb. Roermond 23 december 2009, ECLI:NL:RBROE:2009:BK7698;
Rb. ’s-Gravenhage 21 juli 2010, ECLI:NL:RBSGR:2010:BN1963, CR 2010, 179 m.nt. R.A. Overbeek, *AMI* 2011, p. 14 m.nt. Koelman (Nintendo/Webwinkels);
Rb. Dordrecht 10 augustus 2010, ECLI:NL:RBDOR:2010:BN3858;
Rb. Amsterdam 30 augustus 2010, ECLI:NL:RBAMS:2010:BP1423;
Rb. Zwolle-Lelystad 16 september 2010, ECLI:NL:RBZLY:2010:BR4213;
Rb. Utrecht 30 november 2010, ECLI:NL:RBUTR:2010:BO6823;
Rb. Haarlem 9 februari 2011, ECLI:NL:RBHAA:2011:BP3757 (FTD/Brein);
Rb ‘s-Hertogenbosch 24 februari 2011, ECLI:NL:RBSHE:2011:BP5939;
Rb. Rotterdam 31 maart 2011, ECLI:NL:RBROT:2011:BP9776;
Rb. Rotterdam 20 april 2011, ECLI:NL:RBROT:2011:BQ7167, CR 2011/159 m.nt Van der Hof (BizKey);
Rb. ‘s-Gravenhage 11 mei 2011, IEF 9655 zaak HA ZA 09-414 (G-STAR/Pepsico);
Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5610 (FXP);
Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5615 (FXP);
Rb. ‘s-Gravenhage 11 januari 2012, ECLI:NL:RBSGR:2012:BV0549 (BREIN/Ziggo enX S4All);
Rb. Haarlem 27 januari 2012, ECLI:NL:RBHAA:2012:BW5210;
Rb. Zutphen 22 februari 2012 ECLI:NL:RBZUT:2012:BX1620;
Rb. Amsterdam 12 september 2012 ECLI:NL:RBAMS:2012:BX7043, IER 2013/4 m.nt. J.M.B. Seignette, CR 2013/7 m.nt. A.R. Lodder (Sanoma & Playboy/GS Media; Brit);
Rb. 's-Gravenhage 19 september 2012, ECLI:NL:RBSGR:2012:BX8147;

Rb. Gelderland (militaire kamer) 2 september 2013, ECLI:NL:RBGEL:2013:2802;
Rb. Rotterdam 27 maart 2013, ECLI:NL:RBROT:2013:BZ6071;
Rb. Gelderland 2 oktober 2013, ECLI:NL:RBGEL:2013:6444 (Jager/Jager);
Rb. Amsterdam 12 mei 2014, ECLI:NL:RBAMS:2014:2751, JAR 2014/149 m.nt. C.M. Jakimowicz.

President Rechtbanken (voor 1 jan. 2002) / Voorzieningenrechter (na 1 jan. 2002)

vzr. Rb. Utrecht 12 juli 2005 ECLI:NL:RBUTR:2005:AT9073, Mf oktober 2005, p. 353, m.nt. T.F.W. Overdijk. (BREIN/Kazaa);
vzr. Rechtbank Arnhem, 22 mei 2008, ECLI:NL:RBARN:2008:BD3441 (De Roode Roos);
vzr. Rb. Amsterdam 16 oktober 2008, ECLI:NL:RBAMS:2008:BG0972, Mf 2008-11/12, nr. 39, m.nt Alberdingk Thijm (Bruno Press/Image Media);
vzr. Rb. Roermond 19 februari 2009, ECLI:NL:RBROE:2009:BH2949 (More Entertainment/MyP2P);
vzr. Rb. Amsterdam 22 oktober 2009, ECLI:NL:RBAMS:2009:BK1067 (Brein/Pirate Bay);
vzr. Rb. Amsterdam 14 mei 2013, ECLI:NL:RBAMS:2013:CA0350 (Brein/ING);
vzr. Rb. Amsterdam 21 juli 2014, ECLI:NL:RBAMS:2014:4360 (NUV/Tom Kabinet);
vzr. Rb. Amsterdam 28 januari 2015, IEF 14603 (Belirex/UPC).

BELGIË

Grondwettelijk hof

Arbitragehof 30 april 1997, BS 19 juni 1997;
GwH 22 december 2010, RABG 2011/8, m.nt. F. Schuerman;
GwH 27 juli 2011, nr. 139/2011.

Hof van Cassatie

Cass. 12 maart 1923, Pas. 1923, I, 223;
Cass 10 december 1923, Pas. 1924, 1, 66;
Cass. 2 maart 1956, A.C. 1956, 534;
Cass. 29 oktober 1962, Pas. 1963, 1, p. 272; RW 1963-64, p. 815;
Cass. 11 december 1969. A.C. 1970, 357;
Cass. 2 december 1971, Pas. 1972, I, 323;
Cass. 10 april 1979, A.C. 1978-79, 953;
Cass. 25 oktober 1979, A.C. 1979-80, 261;
Cass. 22 juli 1981, A.C. 1980-81, 646;
Cass. 7 oktober 1981, A.C. 1981-82, 1983;
Cass. 17 juni 1983, A.C. 1982-83, 1290;
Cass. 21 februari 1984, A.C. 1983-84, 347;
Cass. 29 mei 1984, A.C. 1984-1985, 1274;
Cass. 11 december 1984, A.C. 1984-85, 277;
Cass. 18 april, 1985, A.C. 1984-85, 1102;
Cass. 13 mei 1986, A.C. 1985-1986, 558 (Belofte Belasting-ambtenaar);
Cass. 19 mei 1987 A.C. 1986-87, 544, RW 1987-88, 675, m.nt. Verstraeten;
Cass. 12 november 1987, A.C. 1987-88, 325, RW 1987-88, 1379, m.nt. J.L.;
Cass. 26 oktober 1988, A.C. 1988-89, 115;
Cass. 27 februari 1989. A.C. 1988-89, 735;
Cass. 17 januari 1990, A.C. 1989-90, 130, Pas.1990, I, 588, RW 1990-1991, 14, p. 463-464, m.nt. L.Huybrechts, RDPC 1990, 653 (Dutry);
Cass. 19 juni 1990, A.C. 1989-90, 609;
Cass. 9 oktober 1990, A.C. 1990-1991, 68;

Cass. 17 januari 1991, RDPC 1992, 104;
Cass 17 april 1991, A.C. 1990-91, 834, Pas. 1991, I, 736, RW 1991-92, 403, m.nt. A. Vandepas, RDPC 1992, p. 94-101 m.nt. C. De Valckeneer (Druart/Frejdun);
Cass. 26 september 1991, A.C. 1991-92, 97;
Cass. 18 december 1991, JLMB, 1992, 473;
Cass. 24 december 1991, RW 1991-92, 1062, m.nt. M. De Swaef;
Cass., 21 januari 1992, A.R. 1992, 5332;
Cass. 10 november 1992, A.C. 1992, 726;
Cass. 30 juni 1993, Pas. 1993, 635;
Cass. 4 januari 1994, A.C. 1994, I, 1, RW 1994-1995, 187 m.nt. F. D'hont, Rec. Cass 1994, p. 72-75 m.nt. Ph Traest;
Cass. 4 januari 1994, RW 1993-1994, 1054, m.nt. A Vandeplas;
Cass. 9 november 1994, JT 1995, 214;
Cass. 28 februari 1995, A.C. 1995, 117;
Cass. 18 april 1995, A.C. 1984-85, 1102;
Cass 30 mei 1995, A.C. 1995, No 267, JLMB 1998, 488 m.nt. F. Kuty;
Cass. 25 april 1996, A.C. 1996, Cass, 2 maart 2011, RDPC 2011, 893;
Cass. 12 november 1997, RDPC 1998, 586;
Cass. 9 december 1997, A.C. 1997, 542, RW 1997-98, 1441;
Cass. 17 december 1998, A.C. 1998, 1141, RW 1998-99, 1144, m.nt. F. Swennen;
Cass. 21 april 1999, A.C. 1999, 231;
Cass. 17 september 1999, A.C. 1999, 1119;
Cass 3 november 1999, TSR 2000, 255, m.nt. J. Meese;
Cass. 7 december, A.C. 1999, 665, T. Strafrecht, 2000, 161;
Cass. 14 januari 2000, A.C. 2000, 109;
Cass. 8 februari 2000, JLMB 2000, 625 m.nt. A. Sadzat;
Cass. 12 april 2000, RW 2000-2001, 306, m.nt. De Smet;
Cass. 25 september 2000, A.C. 2000, 1424, P&B 2001, 114, m.nt. B. Allemeersch;
Cass. 20 december 2000, A.C. 2000, 714;
Cass. 27 februari 2001, A.J.T. 2000-01, 949, m.nt. I. Verhelst, CR 2001, 202; J. Dumotier, RW 2001-02, 1171; P. Humblet en Vigiles 2001, 153, m.nt. P. De Hert;
Cass. 26 maart 2001, A.C. 1990-91, 400;
Cass. 10 mei 2001, AR C.99.0355.F, A.C. 2001, 270;
Cass. 10 mei 2001, Pas. 2001, I, 807;
Cass. 5 maart 2002, Verkeersrecht 2002, 185;
Cass. 11 maart 2002, Pas. 2002, I, 690;
Cass. 25 september 2003, RW 2003-2004, 1179;
Cass. 14 oktober 2003, P.030762.N, A.C. 2003, 1856 (of 1862?); NjW 2003, 1367, m.nt. E. Brewaeys; RABG 2004, 333, m.nt. F. Schuermans (2004a); RCJB 2004, 405, m.nt. F. Kuty (2004); RDPC 2004, 617; RW 2003-04, 814; T. Strafr. 2004, 129, m.nt. P. Traest; Viliges (N) 2004/1, 15, m.nt. F. Schuermans (2004b) (Antigoon);
Cass. 23 maart 2004, P.04.0012.N, RABG 2004, 1061, m.nt. F. Schuermans (2004c) RDPC 2005, 661 m.nt. C. De Valkeneer Cass. 2 maart 2005, P.04.1644.F, Arr.Cass. 2005, 506, JLMB 2005, 1086 m.nt. M. Beernaert, Journal Proc. 2005, 499, 23, m.nt. P. Toussaint; CR 2005/41, p. 258-263, m.nt. Van Eecke en B. Ooma. (Chocolatier Manon; Antigoon II);
Cass. 2 september 2004, NJW 2004, 953, RW 2004, 5, m.nt. C. Clijmans;
Cass. 16 november 2004 (twee arresten, P.04.1127.N & P.04.0644.N), RABG 2005, 504, m.nt. F. Schuermans, T. Strafr. 2005, 285, m.nt. R. Verstraeten en S. De Decker; Vigiles (N) 2004, 171, m.nt. F. Schuermans (Antigoon III);
Cass. 16 december 2004, AR C030407N;

Cass. 14 januari 2005, NJW 2005, 699, m.nt. E. Brems, RCJB 2006, m.nt J. Van Drooghenbroeck en S. Van Drooghenboeck;
Cass. 2 maart 2005, P. 041644F, ECLI:NL:XX:2005:BM0532, CR 2005, 258, m.nt. P. Van Eecke en B. Ooms, JT 2005, 211, JLMB. 2005, 1086, m.nt. M. Beernaert; Journ. proc. 2005, n° 499, 23, m.nt. P. Toussaint; RABG 2005, 1161, m.nt. S. Berneman, RDPC 2005, 668, m.nt. C. De Valkeneer; (Antigoon IV; Chocolatier; winkelkassa);
Cass. 25 mei 2005, JLMB. 2005, 1408, JT 2005, 481, *RDPC* 2005, 1297;
Cass. 12 oktober 2005, P. 05.0119.F; T. Strafr. 2006, 25, m.nt. F. Verbruggen; Vigiles 2006, 105, m.nt. S. Vandromme, JT 2006, JLMB 2006, 585;
Cass. 19 oktober 2005, AR p.05.1287.F;
Cass. 8 november 2005, P 051106N RABG 2006, 930, m.nt. S. Berneman, 'Onbehoorlijk overheidsoptreden bij bewijsgaring: de kinderen van Antigoon leren de les', *RDPC* 2006, 672, T. Strafr. 2006, 85; Viliges (N) 2006, 22, m.nt. F. Schuermans, 'Reality-televisie, politie en strafvordering: een onmogelijke combinatie?';
Cass. 31 oktober 2006;
Cass. 21 november 2006, P. 060806.N;
Cass. 19 juni 2007, RABG 2008/7, m.nt . F. Van Volsem;
Cass. 20 november 2007, P.07.1173.N/4;
Cass. 22 januari 2008, NC 2008, 140;
Cass. 10 maart 2008, S.07.0073.N, JLMB 2009, 580, m.nt. R. De Baerdemaeker, NjW 2010, 195, m.nt. K. Van Kildonck;
Cass. 2 april 2008, AR P. 07.1744.F, JT 2008, 390, m.nt. F. kuyt;
Cass. 18 april 2008, C.07.0409.F;
Cass. 4 juni 2008, P.08.0489;
Cass. 23 september 2008, AR, P. 08.0519.N, TSR 2009, 151, m.nt. F. Schuermans;
Cass. 23 oktober 2008, Pas. 2008, 2351;
Cass. 10 november 2008, S.06.0029.F, JTT 2009, 18;
Cass. 26 november 2008, RW 2010-11;
Cass. 16 december 2008 P.2008.1210.N;
Cass. 7 mei 2009, A.C. 2009, 1196, 1108;
Cass. 3 september 2009, C.08.0337.N, IRDI 2009, 411, m.nt. M. Buydens;
Cass. 1 oktober 2009, RG C.08.0064.N;
Cass. 17 maart 2010, AR P. 09.1691.F, RW 2011-12, 1332;
Cass. 24 maart 2010, P.10.0407;
Cass. 3 mei 2010, AR. S.009.0024.N;
Cass. 5 oktober 2010, AR P.10.0703.N, T.Strafr. 2011, 66 m.nt. B. Meganck, RW 2011-12, p. 1338, m.nt. R. Saelens en P. De Hert;
Cass. 26 november 2010, PAS, 2010, 3022;
Cass. 21 januari 2011, Pas. 2011, 234;
Cass. 26 januari 2011, AR P. 10.1321.F, *RDPC* 2012, 82, m.nt. D. Dillenbourg, TSR 2011, m.nt. F. Schuermans;
Cass. 2 maart 2011, RDPC 2011, 893;
Cass. 2 mei 2011, JTT 2011, 469;
Cass. 18 mei 2011, AR P.10.2049.F;
Cass. 31 mei 2011, AR P. 10.2037.F, JT 2011, m.nt. M.-A. Beernaert, JLMB 2011, m.nt. A De Nauw;
Cass. 26 januari 2012, C.11.0108.N, IEFBE 150, IRDI, 2012/2 m.nt F. Gotzen;
Cass. 15 juni 2012, AR C.11.0721.F;
Cass. 22 oktober 2013, P.13.0550.N (Telenet, Tecteo en Brutele).

Hoven van Beroep

Hof van Beroep Antwerpen 11 oktober 2000, AM 2000, 357, IRDI 2001, 137 (pornografische versie Jerommeke);

Hof van Beroep Luik 7 mei 2003, AM 2005, 128;
Hof van Beroep Antwerpen 23 mei 2003;
Hof van Beroep Antwerpen 15 juni, 2009, 2008/AR/1087, NJW 2010/225, p. 447;
Hof van Beroep Antwerpen 16 november 2009, NjW 2010, 545;
Hof van Beroep Antwerpen 26 september 2011, RABG 2011/18, 1269;
Hof van Beroep 28 januari 2010, CR, 108, m.nt. B. Bruyndonckx (Sabam/Scarlet);
Hof van Beroep Brussel 19 maart 2013, 2012 CO 674, IEFBE 380 (EBVBA/X).

Arbh. Brussel 3 mei 2006, AR 45.922;
Arbh. Brussel 15 juni 2006, JTT 2006, 392;
Arbh. Antwerpen (afd. Hasselt), 2 september 2008, AR 2070230, onuitg.

Rechtbanken
Corr. Brussel 18 april 1986, RW 1987-88, 60;
Corr. Rb. Verviers 8 november 1989, JLMB. 1990, 717;
Rb. Gent, 6 februari 1992, TGR 1992, 65 (Videobanden);
Corr. Rb. Antwerpen 28 februari 2002, AM 2002, 340;
Corr. Hasselt 3 mei 2002, IRDI 2002, 171;
Corr. Rechtbank Ieper 26 mei 2005, AM 2005, 339, m.nt. J. Ceuleurs;
Corr. Gent 19 oktober 2005, T. Strafr. 2006, p. 42-43, 13;
Vzr. Rb. Brussel 29 juni 2007, CR 2007, 280, m.nt. F. Petillion
Arbrb. Brussel 4 december 2007, JTT 2008, 179;
Arbrb. Gent 1 september 2008, AR 175054/06;
Arbrb. Luik 3 september 2008, AR 371.015;
Corr. rechtbank Dendermonde, 29 maart 2006, T. Strafrecht 2007/2;
Rb. Koophandel Antwerpen 8 juli 2010, A/10/5374, IEF 10292 (BAF/Telenet en Belgacom);
Cor. Rb. Kortrijk, 29 februari 2012, nr. 12/383, IEF 11029; IEFBE 173.

DUITSLAND

Bundesgerichtshof
BGH 12 mei 2010, I ZR 121/08 (Sommer unseres Lebens).

VERENIGDE STATEN

United States Supreme Court
United States Supreme Court 27 juni 2005, 545 U.S. 913 (MGM Studios, Inc./Grokster, Ltd.).

United States Court of Appeals
United States Court of Appeals, 14 februari, 398 F.3d 1193, 10th Cir., 2005 (Palladium Music, Inc./ EatSleepMusic, Inc.).

United States District Court
United States District Court, Central District of California, 18 november 2004, 346 F. Supp. 2d 1068. (2004 WL 2755842) (Warner Bros./Carmine Caridi et al.);
United States District Court of Massachusetts, August 23, 2012, no. 07-111446-RWZSONY (BMG Music Entertainment/Joel Tenenbaum).