

***‘De belangenafweging bij afgifte van naw-gegevens’***

**Toetsing van:**

**Afstudeeronderzoek**

**HBR-4-AS17-AS**

**Aantal woorden:**

**16.354**

**Hogeschool Leiden Opleiding HBO-Rechten**

**Naam en studentnummer Onderzoeksdocent**

Jacobien van der Kooij – S1087900 Mevr. Van Mierlo

**Opdrachtgever** **Afstudeerbegeleider**

Stichting BREIN Mevr. Filemon

Carla de Bruin en

Tim Kuik **Datum**

 16-06-2020

**Klas Collegejaar**

Re4H 2019/2020, blok 15

# Voorwoord

Geachte lezer,

Voor u ligt mijn afstudeeropdracht. Na een lange periode van hard werken en veel lezen is dit het resultaat. Dit onderzoek is uitgevoerd ter afsluiting van mijn opleiding HBO-Rechten aan de Hogeschool Leiden; de afstudeeropdracht is geschreven in opdracht van Stichting BREIN. Dit afstudeeronderzoek heeft betrekking op de afgifte van naam, adres en woonplaats (hierna: naw-gegevens) door usenet-, access- en hostingproviders en richt zich met name op de feiten en omstandigheden waaronder Stichting BREIN deze gegevens succesvol kan opvragen bij de providers.

Ik wil Stichting BREIN daarom bedanken voor haar hulp en geduld gedurende mijn afstudeerperiode. Daarnaast wil ik mevrouw Van Mierlo danken voor haar hulp, geduld en bemoedigende woorden tijdens de gehele fase van het afstudeeronderzoek. Ook gaat mijn dank uit naar mijn afstudeerbegeleider, mevrouw Filemon, voor haar feedback en hulp tijdens het schrijven van mijn afstudeeropdracht. Verder wil ik mijn vrienden en familie bedanken voor hun steun gedurende deze periode.

Hierbij wens ik u veel plezier bij het lezen van mijn afstudeeropdracht.

Jacobien van der Kooij

Alphen aan den Rijn, 16 juni 2020

# Samenvatting

Om inbreuk op de auteursrechten van de aangeslotenen van Stichting BREIN (hierna: BREIN) te kunnen beëindigen, moet BREIN de inbreukmaker kunnen aanspreken op het onrechtmatig handelen. BREIN beschikt echter niet altijd over de naw-gegevens om een inbreukmaker in rechte te kunnen betrekken. Wanneer de inbreuk online plaatsvindt, is hierbij vaak een tussenpersoon betrokken. In dit onderzoek is specifiek gekeken naar usenet-, access- en hostingproviders als tussenpersoon. Deze providers weigeren vaak naw-gegevens vrijwillig af te geven. Dit zou namelijk een inbreuk zijn op de privacy van de klant. In dit onderzoek is onderzocht wanneer providers naw-gegevens dienen af te staan.

Het doel van deze afstudeeropdracht is BREIN te adviseren over onder welke feiten en omstandigheden usenet-, access- en hostingproviders naw-gegevens moeten afstaan bij verondersteld auteursrechteninbreuk. Om antwoord te krijgen op de vraag wanneer BREIN naw-gegevens kan opvragen, is onderzoek verricht door middel van wetsanalyse en literatuuronderzoek. Tevens is jurisprudentieonderzoek uitgevoerd om de afwegingen en beoordelingen van de rechters in kaart te brengen. Uit de analyse is naar voren gekomen welke belangen de rechter het zwaarst vindt wegen bij de belangenafweging en wanneer een provider naw-gegevens dient af te geven.

Een van de belangrijkste bevindingen van de wetsanalyse en het literatuuronderzoek is de rol van het Lycos/Pessers-arrest. Aan de hand dit arrest is een viertal criteria opgesteld waaraan moet worden voldaan voor afgifte van naw-gegevens aan een derde door een tussenpersoon. Het eerste criterium is dat de informatie aannemelijk onrechtmatig en schadelijk is. Het tweede is dat de benadeelde partij een reëel belang heeft bij afgifte van de naw-gegevens. Het derde criterium is dat er geen minder ingrijpende mogelijkheden zijn. Het laatste criterium houdt in dat het belang van de benadeelde prevaleert boven dat van de inbreukmaker en de provider. Bij de belangenafweging staan de volgende belangen tegenover elkaar:

* het recht op bescherming van eigendom;
* het recht op bescherming van persoonsgegevens;
* het recht op eerbiediging van het privéleven;
* de vrijheid van meningsuiting;
* de vrijheid van ondernemerschap.

Naast de criteria van het Lycos/Pessers-arrest is het van belang dat BREIN persoonsgegevens rechtmatig verwerkt. BREIN moet daarom aan haar verantwoordingsplicht voldoen die volgt uit de Algemene verordening gegevensbescherming.

De belangrijkste resultaten van het jurisprudentieonderzoek zijn hoe de rechter de verschillende belangen tegen elkaar afweegt. Hieruit volgt dat een rechthebbende duidelijk moet maken welke juridische stappen hij gaat nemen als hij de naw-gegevens heeft ontvangen. Verder is het van belang hoe ernstig de inbreuk is en of er sprake is van een meervoudige of enkelvoudige inbreuk. Bij de belangenafweging wordt de vrijheid van meningsuiting vaak buiten beschouwing gelaten. Het is verder van belang dat BREIN aan haar zorgvuldigheidsverplichting voldoet die voortvloeit uit de Algemene verordening gegevensbescherming.

BREIN kan naw-gegevens opvragen bij een usenet-, access- of hostingprovider op basis van art. 6:162 Burgerlijk Wetboek in combinatie met het Lycos/Pessers-arrest of via een rechterlijk bevel, blijkens art. 28 lid 9 Auteurswet. Wanneer BREIN kiest voor de directe weg naar de provider, moet deze provider op basis van de zorgvuldigheidsplicht die op hem rust zelf de belangenafweging maken. Echter, de provider kan beoordelen dat het belang van de provider of dat van de inbreukmaker zwaarder weegt, waardoor BREIN alsnog een rechtszaak moet aanspannen. Daarnaast kan de inbreukmaker gebruikmaken van het recht van bezwaar, waardoor het proces tot het verkrijgen van de naw-gegevens voor BREIN langer duurt.

De andere mogelijkheid is dat BREIN direct naar de rechter stapt voor een rechterlijk bevel om naw-gegevens te verkrijgen van een provider. Via deze weg kan BREIN eventueel sneller de naw-gegevens verkrijgen. Verder laat de rechter bij deze mogelijkheid het recht op bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven buiten beschouwing.

BREIN heeft dus twee mogelijkheden om aan naw-gegevens te komen van inbreukmakers bij usenet-, access- en hostingproviders. Beide mogelijkheden hebben hun voordelen en nadelen.

Inhoudsopgave

[Voorwoord 2](#_Toc43037885)

[Samenvatting 3](#_Toc43037886)

[1. Inleiding 7](#_Toc43037887)

[1.1 Probleemanalyse 7](#_Toc43037888)

[1.2 Doelstelling 12](#_Toc43037889)

[1.3 Vraagstelling 12](#_Toc43037890)

[1.4 Onderzoeksmethode 12](#_Toc43037891)

[1.4.1 Deelvraag 1 12](#_Toc43037892)

[1.4.2 Deelvraag 2 13](#_Toc43037893)

[1.4.3 Deelvraag 3 13](#_Toc43037894)

[1.5 Leeswijzer 14](#_Toc43037895)

[2. Juridisch kader 15](#_Toc43037896)

[2.1 Stichting BREIN 15](#_Toc43037897)

[2.2 Providers 16](#_Toc43037898)

[2.2.1 Tussenpersoon 16](#_Toc43037899)

[2.3 Auteursrecht 17](#_Toc43037900)

[2.3.1 Openbaar maken 18](#_Toc43037901)

[2.3.2 Verveelvoudigen 19](#_Toc43037902)

[2.3.3 Ontwikkelingen 19](#_Toc43037903)

[2.4 Handhaving 20](#_Toc43037904)

[2.5 Strafrechtelijke vervolging 21](#_Toc43037905)

[2.6 Rechterlijk bevel 21](#_Toc43037906)

[2.7 Onrechtmatige daad 22](#_Toc43037907)

[2.8 Lycos/Pessers-arrest 22](#_Toc43037908)

[2.9 Belangenafweging 23](#_Toc43037909)

[2.10 Algemene verordening gegevensbescherming 25](#_Toc43037910)

[2.10.1 Rechtmatigheid van verwerking 26](#_Toc43037911)

[2.10.2 Verantwoordingsplicht 26](#_Toc43037912)

[2.10.3 Recht van bezwaar 27](#_Toc43037913)

[2.10.4 Recht op gegevenswissing 28](#_Toc43037914)

[2.11 Conclusie 29](#_Toc43037915)

[3. Einde van een tijdperk? 30](#_Toc43037916)

[3.1 Lycos/Pessers-arrest 30](#_Toc43037917)

[3.1.1 Rechtsregel 30](#_Toc43037918)

[3.1.2 Gevolgen 31](#_Toc43037919)

[3.2 Promusicae-arrest 31](#_Toc43037920)

[3.2.1 Rechtsregel 31](#_Toc43037921)

[3.3 Reactie van Ministerie van Justitie en Veiligheid 32](#_Toc43037922)

[3.4 Bonnier Audio-arrest 32](#_Toc43037923)

[3.4.1 Rechtsregel 32](#_Toc43037924)

[3.5 Nederlandse rechter 33](#_Toc43037925)

[3.6 Conclusie 33](#_Toc43037926)

[4. Resultaten 34](#_Toc43037927)

[4.1 Recht op bescherming van eigendom 34](#_Toc43037928)

[4.2 Recht op privacy 36](#_Toc43037929)

[4.3 Vrijheid van meningsuiting 38](#_Toc43037930)

[4.4 Vrijheid van ondernemerschap 39](#_Toc43037931)

[4.5 Prevalerend belang 40](#_Toc43037932)

[4.6 Bijzonderheden 41](#_Toc43037933)

[4.7 Conclusie 43](#_Toc43037934)

[5. Conclusie 44](#_Toc43037935)

[6. Aanbevelingen 46](#_Toc43037936)

[7. Bronnenlijst 48](#_Toc43037937)

[Bijlage 54](#_Toc43037938)

# Inleiding

## 1.1 Probleemanalyse

In 2017 heeft 37% van de mensen met internettoegang illegale content gedownload. Dit betekent dat zij iets hebben gedownload zonder hiervoor te betalen of zonder toestemming van de rechthebbende van het werk.[[1]](#footnote-1) In Nederland is het peer-to-peer-protocol BitTorrent de populairste manier om illegaal gebruik te maken van entertainmentcontent. Uit een studie van Sandvine in 2018 is gebleken dat 97% van het uploadverkeer gebruikmaakt van BitTorrent.[[2]](#footnote-2)

Niet iedere illegale download of stream is een gemiste verkoop voor de auteursrechthebbende. Wanneer een consument voor de content moet betalen, zal hij alleen kopen wat hij wil zien. Wanneer de content gratis beschikbaar is, is hij echter minder kritisch. Hierdoor is hij eerder geneigd de content te bekijken of te beluisteren, ook als deze niet in zijn voorkeursgenre valt. Onderzoek van Considerati in samenwerking met het Instituut voor Informatierecht, het onderzoekinstituut CentERdata en online merken beschermer MarkMonitor heeft getoond dat voor iedere 10 illegale downloads of streams er 3,2 films minder legaal gekocht worden. Dit betekent dat niet al deze 10 consumenten de film zouden kopen die zij wel gratis kunnen downloaden of streamen.[[3]](#footnote-3)

De schade die het illegale gebruik van BitTorrent veroorzaakt, beperkt zich niet tot audiovisuele producten. Ook de rechtmatige exploitatie van muziek, games en e-books heeft te lijden onder illegaal gebruik. Uit onderzoek van Radar naar de manier waarop mensen aan e-books komen, is gebleken dat bijna de helft van de panelleden deze kopieert via bekenden en dat 17% ze zelf illegaal downloadt.[[4]](#footnote-4) Daarnaast gebruikt 35% van de internettende consumenten illegale bronnen voor muziek.[[5]](#footnote-5)

Om de inbreuk op auteursrechten te beëindigen, is in Nederland Stichting BREIN (hierna: BREIN) actief. BREIN bestrijdt intellectueel-eigendomsfraude namens auteurs, uitvoerende kunstenaars, uitgevers, producenten en distributeurs van muziek, film, video, boeken en andere geschriften, games en interactieve software.[[6]](#footnote-6) BREIN behartigt de belangen van aangeslotenen die vallen onder het auteursrecht en de naburige rechten.

In dit onderzoek is alleen het auteursrecht bekeken. Auteursrecht is het uitsluitende recht van de maker van een werk ten aanzien van de waarneembare vorm van zijn werk. Hierbij is ‘werk’ immaterieel bedoeld, als de geestelijke schepping die zich manifesteert in de uiterlijk waarneembare verschijningsvorm.[[7]](#footnote-7) Hoewel het intellectueel-eigendomsrecht tot het burgerlijk recht behoort, is het niet geregeld in het Burgerlijk Wetboek (hierna: BW),[[8]](#footnote-8) maar in bijzondere wetten en internationale verdragen. In Nederland is de belangrijkste wet de Auteurswet (hierna: Aw). Volgens art. 1 Aw geeft het auteursrecht de maker, de uitsluitende bevoegdheid het werk openbaar te maken en te verveelvoudigen.[[9]](#footnote-9) Op basis van de Aw is inbreuk op auteursrecht strafbaar; dit is te vinden in art. 31 Aw, jo. art. 31a Aw. De handhaving van auteursrechten is hoofdzakelijk een civielrechtelijke aangelegenheid.[[10]](#footnote-10) BREIN beschermt de auteursrechten van haar aangeslotenen daarom op civielrechtelijk niveau.

Art. 2 van de statuten van BREIN geeft de volgende definitie van aangeslotene: ‘*Iedere natuurlijke of rechtspersoon die een bedrijf uitoefent dat bestaat uit de rechtmatige exploitatie van informatie of informatiedragers en iedere rechtspersoonlijkheid hebbende organisatie die de belangen behartigt van rechthebbenden op informatie of rechtmatige exploitanten of wier doelstelling op enigerlei wijze daarmee direct of indirect verband houdt en als zodanig door het bestuur van de Stichting is toegelaten.*’ De aangeslotenen van BREIN dragen ook bij aan het vermogen, volgens art. 4 sub a van de statuten van BREIN.

BREIN handhaaft onder andere op vraag- en aanbodsites, zoals Marktplaats, en op illegale websites, zoals usenet. Dit laatste is een online-platform voor het uitwisselen van digitaal materiaal, zoals teksten, foto’s, films, e-books en muziekbestanden. Gebruikers van usenet kunnen hierop materiaal plaatsen door bestanden naar usenet te uploaden (‘posten’) en deze daarna in nieuwsgroepen te plaatsen. Andere gebruikers kunnen deze bestanden vervolgens uit de nieuwsgroepen downloaden. Om toegang tot het materiaal op usenet te krijgen, dient een abonnement afgesloten te worden bij een commerciële usenetprovider, zoals NSE, XS News en Newsconnection.

Het is op dit moment lastig om de bestanden op usenet zelf te vinden. Het werk wordt opgedeeld in verschillende NZB-bestanden, die geen herleidbare naam hebben. De uploader weet als enige welke NZB-bestanden tot het werk behoren. De NZB-bestanden worden samengevoegd als ‘spot’. Als iemand de spot downloadt, downloadt hij het gehele werk. De uploader koppelt de bestanden voor een spot zelf; de spot heeft wel de naam van het werk. De spots zijn te vinden op (verschillende) spotwebsites. Op deze manier maken uploaders de door hen geplaatste content eenvoudig toegankelijk voor derden.

Wanneer BREIN een uploader wil aanspreken, moet ze onderzoek verrichten naar de activiteiten van die uploader. Hiervoor moeten de naam, adres en woonplaats (hierna: naw-gegevens) van de uploader achterhaald worden. Een onderzoek naar een uploader op een illegale website kan vastlopen wanneer er onvoldoende aanknopingspunten zijn, bijvoorbeeld:

* betaalgegevens om te doneren op een illegale website ontbreken;
* persoonlijke informatie ontbreekt;
* geen koppeling kunnen maken aan een bestaand persoon zijn naw-gegevens.

De uploads van de inbreukmaker bij de door hem gebruikte usenetprovider zijn bij onvoldoende aanknopingspunten het enige spoor. In dat geval sommeert BREIN de desbetreffende provider. BREIN vraagt in haar sommatie of de provider het verzoek wil doorsturen naar de uploader en verzoekt daarnaast de naw-gegevens van deze klant af te geven. Op deze wijze krijgt de inbreukmaker de mogelijkheid om de zaak zelf te schikken met BREIN, wat voor BREIN mogelijk kosten bespaart. Wanneer BREIN alleen het verzoek tot afgifte van de naw-gegevens doet bij de provider, bestaat de kans dat de provider dit verzoek afwijst; dan moet BREIN een rechtszaak starten tegen de provider om de naw-gegevens te verkrijgen. De provider wil die gegevens niet altijd verstrekken, omdat dit inbreuk zou maken op de privacy van diens klant. In dit geval kan de inbreukmaker niet aangesproken worden en kan hij ongestoord verder gaan. Verschillende providers willen de gevraagde naw-gegevens niet vrijwillig aan BREIN afgeven. Hierdoor ontstaat een probleem voor BREIN en haar aangeslotenen.[[11]](#footnote-11)

BREIN is volgens haar statuten en in samenhang met art. 3:305a BW bevoegd om rechtsvorderingen in te stellen ten behoeve van rechthebbenden. BREIN doet dit voor haar aangeslotenen en hun leden. Wanneer BREIN naw-gegevens vordert van een provider, is dit op basis van de onrechtmatige daad. De onrechtmatige daad is geregeld in art. 6:162 BW. Als onrechtmatige daad wordt op grond van art. 6:162 lid 2 BW ‘*aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt’*.[[12]](#footnote-12) Een onrechtmatige daad is te vertalen naar het, door een handelen of nalaten, schenden van een gedragsnorm die in onze maatschappij geldt.[[13]](#footnote-13)

Wanneer BREIN naw-gegevens opvraagt bij een provider op basis van art. 6:162 lid 2 BW, doet ze dit op grond van het Lycos/Pessers-arrest.[[14]](#footnote-14) Dit arrest uit 2005 bevat een belangrijke uitspraak over de afgifte van naw-gegevens en wordt door rechters veelal gebruikt om het vraagstuk van afgifte van naw-gegevens door tussenpersonen te beoordelen. Postzegelhandelaar en advocaat Pessers verkocht op eBay postzegels. Pessers werd van fraude beschuldigd op een gratis website van internetserviceprovider (hierna: isp) Lycos en spande daarop een kort geding aan tegen Lycos om achter de naam en het adres van de persoon te komen die Pessers beschuldigde.

De Hoge Raad heeft in dit arrest bepaald dat onder bepaalde omstandigheden de rechtsplicht tot afgifte van de naw-gegevens aan een derde kan bestaan. Hierbij heeft de Hoge Raad de volgende vier criteria vastgesteld voor de afgifte van naw-gegevens door isp’s:

1. De informatie is redelijkerwijs aannemelijk onrechtmatig en schadelijk.
2. De eiser heeft een reëel belang bij afgifte.
3. Er zijn geen minder ingrijpende mogelijkheden.
4. Afweging van de betrokken belangen van de eiser, de provider en de inbreukmaker brengt mee dat het belang van de eiser behoort te prevaleren.[[15]](#footnote-15)

Hiervan is het vierde criterium het lastigst.[[16]](#footnote-16) Dit criterium is namelijk een belangenafweging. In de praktijk wordt vaak gekeken naar de belangen van de eiser en de inbreukmaker. Hierbij staan verschillende rechten tegenover elkaar. Aan de ene kant staat het recht op bescherming van eigendom, met inbegrip van intellectueel eigendom (art. 17 lid 2 Handvest van de grondrechten van de Europese Unie [hierna: Handvest]). Aan de andere kant staan de volgende rechten:

* het recht op bescherming van persoonsgegevens (art. 8 Handvest);
* het recht op eerbiediging van het privéleven (art. 7 Handvest);
* de vrijheid van meningsuiting (art. 11 Handvest);
* de vrijheid van ondernemerschap (art. 16 Handvest).

Het Handvest is in dit onderzoek gebruikt, omdat het steeds meer invloed heeft op het recht op bescherming van intellectueel eigendom.[[17]](#footnote-17)

Rechters zijn echter niet altijd consistent met de toepassing van het Lycos/Pessers-arrest, vanwege het Promusicae-arrest en het Bonnier Audio-arrest.[[18]](#footnote-18) [[19]](#footnote-19) Desondanks wordt het Lycos/Pessers-arrest[[20]](#footnote-20) nog steeds gebruikt in de rechtspraak en is de vierstappentoets het relevantste toetsingskader. Dit wordt verder besproken in Hoofdstuk 3.

Bij afgifte van naw-gegevens is de privacy van de inbreukmaker relevant. Sinds 25 mei 2018 geldt in de Europese Unie (hierna: EU) nieuwe regelgeving voor de verwerking van persoonsgegevens. Dit is Verordening 2016/679, Algemene verordening gegevensbescherming (hierna: AVG). De AVG heeft de privacyrechten van de betrokkene versterkt en uitgebreid. Tevens heeft de tussenpersoon meer verplichtingen gekregen.[[21]](#footnote-21)

Een van de beginselen van de AVG is dat het verwerken van persoonsgegevens rechtmatig moet zijn.[[22]](#footnote-22) In het kader van het onderhavige vraagstuk is de verwerking van persoonsgegevens noodzakelijk voor BREIN om de gerechtvaardigde belangen voor haar aangeslotenen te kunnen behartigen. Deze grondslag kan alleen gebruikt worden volgens art. 6 sub f AVG wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van de verhouding met de verwerkingsverantwoordelijke.[[23]](#footnote-23)

Een ander belangrijk aspect dat volgt uit de invoering van de AVG, is dat de (mogelijke) inbreukmaker het recht van bezwaar heeft gekregen. Dit recht is beschreven in art. 21 lid 1 AVG. Voordat gegevens worden verwerkt, moet de betrokkene op de hoogte worden gebracht. Hij heeft dan de mogelijkheid om bezwaar te maken. Uit dit recht van bezwaar volgen het recht op beperking van de verwerking (art. 18 AVG) en het recht op gegevenswissing (art. 17 AVG).

Een recent en bekend voorbeeld van een zaak over afgifte van naw-gegevens is de zaak van Dutch FilmWorks (hierna: DFW) tegen Ziggo.[[24]](#footnote-24) DFW is distributeur van verschillende films in Nederland, zoals ‘The Hitman’s Bodyguard’, en wil illegale downloaders aanpakken. DFW verzamelde de IP-adressen van 377 mensen die te vinden waren op BitTorrent-netwerken en die ‘The Hitman’s Bodyguard’ hadden gedownload. DFW verzocht daarna Ziggo opgave te doen van de naw-gegevens van 174 IP-adressen. Ziggo antwoordde dat het de gegevens bewaarde, maar dat het de naw-gegevens niet vrijwillig wilde afstaan.

Volgens Ziggo beschikte het niet meer over 74 IP-adressen door een technisch probleem. Ziggo beschikte nog wel over de overige 100 IP-adressen die DFW had verzocht. Het bedrijf wilde de gegevens van de overige IP-adressen niet vrijwillig afgeven, omdat het onvoldoende wist of klanten inbreuk hadden gemaakt op de rechten van de film van DFW. Als dit het geval was, had Ziggo te weinig informatie over welke klanten dit dan waren geweest. DFW deed als antwoord hierop een aanvullend verzoek tot afgifte, maar Ziggo wees ook dit verzoek af. Uiteindelijk heeft de rechter over deze kwestie moeten oordelen.

De rechter gaf DFW op verschillende punten gelijk. Hij stelde vast dat een film niet illegaal mag worden gedownload of geüpload en dat de distributeur een belang heeft bij het verkrijgen van de naw-gegevens die bij de IP-adressen horen. Ook constateerde de rechter dat de houder van een internetaansluiting weliswaar niet de inbreukmaker zelf hoeft te zijn, maar dat dit een belang voor DFW bij afgifte van de gegevens niet in de weg staat. Na de belangenafweging besloot de rechter dat Ziggo de naw-gegevens niet hoefde af te staan. De rechter oordeelde dat het om een eenmalige inbreuk ging en dat er geen aanleiding was te veronderstellen dat de persoon achter een specifiek IP-adres ook betrokken is bij andere illegale downloads. Hiernaast had DFW onvoldoende duidelijk gemaakt op welke wijze hij de IP-adreshouders wilde benaderen. DFW wist nog niet of hij de IP-adreshouder kon aanmerken als downloader of dat iemand anders op het adres aansprakelijk is. Het was ook onduidelijk of een voor te stellen schikkingsbedrag overeenkwam met de feitelijke schade. Verder was het niet duidelijk wat DFW aan de IP-adreshouder zou meedelen omtrent de rechten en plichten van IP-adreshouders.[[25]](#footnote-25) De rechter oordeelde daarom dat het belang van Ziggo zwaarder woog dan het belang van DFW.[[26]](#footnote-26)

In hoger beroep oordeelde het Gerechtshof wederom in het nadeel van DFW, omdat de distributeur opnieuw niet transparant was in welke actie hij tegen de houders van de IP-adressen ging nemen. Zowel in zijn pleidooi als in het protocol dat hij had ingediend bij de Autoriteit Persoonsgegevens was DFW niet transparant.[[27]](#footnote-27) Dit kwam vooral doordat het onzeker was of de betrokken Ziggoklant ook daadwerkelijk de inbreukmaker was. Hierdoor zou het evenwicht van belangen verstoord worden. Ziggo kon zijn klanten niet correct inlichten over de gevolgen van de gegevensverstrekking aan DFW, al zou dit wel moeten volgens artt. 5 en 14 lid 4 AVG. Voordat een Ziggoklant geconfronteerd kan worden met een maatregel, moet hem de gelegenheid zijn geboden om het gebruik van zijn internetaansluiting te onderzoeken en zijn rol daarin vast te stellen.

Hiernaast was DFW onvoldoende transparant over onder welke omstandigheden hij welke bedragen van Ziggoklanten zou vorderen. Aangezien DFW de hoogte van de vordering niet voldoende inzichtelijk had gemaakt, kon niet worden getoetst of de voorgenomen maatregelen in een redelijke verhouding stonden tot het belang dat daarmee voor DFW werd gediend en het privacybelang van de Ziggoklant.[[28]](#footnote-28) Door het ontbreken van de mogelijkheid om een evenwichtige afweging van belangen te kunnen maken, kon er geen sprake zijn van prevalerende belangen van DFW, zoals gesteld in het vierde criterium bij het Lycos/Pessers-arrest.[[29]](#footnote-29)

Het vierde criterium luidt: ‘Afweging van de betrokken belangen van de eiser, de provider en de inbreukmaker brengt mee dat het belang van de eiser behoort te prevaleren’. Vaak zijn de eerste drie criteria eenvoudig uit te leggen en te bewijzen, maar de belangenafweging is niet altijd eenduidig.

## 1.2 Doelstelling

Het doel van deze afstudeeropdracht is om BREIN te adviseren over onder welke feiten en omstandigheden usenet-, access- en hostingproviders naw-gegevens moeten afstaan bij auteursrechteninbreuk.

## 1.3 Vraagstelling

*Centrale vraag*

Wat kan aan Stichting BREIN worden geadviseerd met betrekking tot de afgifte van naw-gegevens door usenet-, access- en hostingproviders, blijkens wet- en regelgeving, literatuuronderzoek en jurisprudentieonderzoek?

*Theoretisch-juridische deelvragen*

1. In welke gevallen kan BREIN naw-gegevens opvragen, blijkens wet- en regelgeving en literatuuronderzoek?
2. In hoeverre geldt de rechtspraak in het Lycos/Pessers-arrest nog na diverse toetsingen, door zowel politiek als in de hogere rechtspraak, betreffende het verschaffen van naw-gegevens door usenet-, access- en hostingproviders, blijkens wet- en regelgeving en literatuuronderzoek?

*Praktijkgerichte deelvraag*

1. Onder welke feiten en omstandigheden besluit de rechter welke belangen zwaarder wegen bij de belangenafweging die volgt uit het Lycos/Pessers-arrest, blijkens jurisprudentieonderzoek?

## 1.4 Onderzoeksmethode

### 1.4.1 Deelvraag 1

Voor de eerste deelvraag was gekeken naar de bestaande wet- en regelgeving en literatuur. Voor het literatuuronderzoek waren meerdere bronnen geraadpleegd. Van elke bron was de recentste versie gebruikt. Al dit onderzoek is verricht om een zo compleet mogelijk beeld te krijgen van de situaties waarin BREIN rechtmatig naw-gegevens mag opvragen.

Voor het beantwoorden van deze eerste deelvraag was ook gebruikgemaakt van het Handvest. Dit is een bijlage van het verdrag van Lissabon, dat niet geaccepteerd is door Nederland. Het Handvest heeft gelding binnen de rechtsorde van de lidstaten en hierdoor ook in Nederland.[[30]](#footnote-30) Het Hof van Justitie van de Europese Unie (hierna: Hof van Justitie) past sinds 2008 steeds vaker het Handvest toe. Deze toepassing ziet toe op de invulling van intellectueel-eigendombegrippen, bij het bepalen van de reikwijdte van beperking op exclusieve rechten en bij het stellen van grenzen aan de handhaving. De belangrijkste grondrechten zijn het recht op privacy, de vrijheid van meningsuiting en de vrijheid van ondernemerschap. Het Hof van Justitie gebruikt in zijn arrest de grondrechten zoals vastgelegd in het Handvest vooral als interpretatiemiddel.[[31]](#footnote-31)

### 1.4.2 Deelvraag 2

Het Lycos/Pessers-arrest is een standaardarrest dat gebruikt wordt voor de afgifte van naw-gegevens door tussenpersonen.[[32]](#footnote-32) Door twee uitspraken van het Hof van Justitie werd echter gedacht dat dit arrest niet langer als norm zou dienen.[[33]](#footnote-33)

Voor het beantwoorden van deelvraag 2 was bekeken wat er na het Lycos/Pessers-arrest door verschillende rechters is bepaald.[[34]](#footnote-34) Hiervoor was niet alleen de betreffende literatuur geraadpleegd, maar ook de verschillende uitspraken van het Hof van Justitie. Voor deze standaardjurisprudentie was onderzocht hoe deze van toepassing is en hoe het Hof van Justitie erover oordeelt. Voor de implementatie van de uitspraken waren twee uitspraken van de Nederlandse rechters bekeken; hierbij werd de rest van de uitspraak niet beoordeeld.

### 1.4.3 Deelvraag 3

Na de beantwoording van de theoretisch-juridische deelvragen was duidelijk geworden wanneer usenet-, access- en hostingproviders naw-gegevens moeten afstaan. Deze informatie kon worden meegenomen naar het praktijkgerichte onderzoeksgedeelte. Een essentieel onderdeel van dit onderzoek was de interpretatie van de rechter. Het was van groot belang vast te stellen hoe zwaar de rechter de verschillende belangen afweegt om te bepalen of de provider naw-gegevens moet afstaan. Om deze deelvraag te beantwoorden, was een jurisprudentieonderzoek uitgevoerd naar welk belang prevaleert en waarom dit belang prevaleert in de beoordeling van de rechter.

Om deze vraag te beantwoorden, waren alle relevante uitspraken uit de periode 2005-2020 geanalyseerd. Ten behoeve van deze vraag waren vijftien uitspraken aangemerkt als relevant. Deze uitspraken gingen over auteursrechtinbreuk en alle gedaagden zijn usenet-, access- of hostingprovider. De uitspraken waren ook verschenen na het Lycos/Pessers-arrest,[[35]](#footnote-35) en waren het resultaat van een zoekopdracht naar ‘Lycos’, ‘Pessers’ en ‘afgifte naw-gegevens’. Vanwege het anonimiseren van uitspraken waren de zoektermen ‘Lycos’ en ‘Pessers’ apart gebruikt; de naam van Pessers werd niet in elke uitspraak gebruikt. De laatste zoekopdracht naar uitspraken dateert van 1 mei 2020. Verder waren uitspraken gekozen waarin de belangenafweging wordt besproken.

De focus van het jurisprudentieonderzoek lag bij het vierde criterium van het Lycos/Pessers-arrest.[[36]](#footnote-36) Nadat duidelijk werd welke belangen relevant waren en hoe de rechter deze belangen meenam in de overweging, was de analyse van de relevante uitspraken volbracht. Hieruit waren een aantal conclusies getrokken. De betreffende topics waren:

* recht op bescherming van eigendom, met inbegrip van intellectueel eigendom (art. 17 lid 2 Handvest);
* recht op privacy (dit is het recht op bescherming van persoonsgegevens [art. 8 Handvest]);
* recht op eerbiediging van het privéleven (art. 7 Handvest);
* vrijheid van meningsuiting (art. 11 Handvest);
* vrijheid van ondernemerschap (art. 16 Handvest);
* prevalerend belang.

In de analyse was er ook ruimte om bijzonderheden te noteren.

1.5 Leeswijzer

In Hoofdstuk 2 wordt de nadruk gelegd op de relevante wet- en regelgeving en literatuur omtrent de afgifte van naw-gegevens van providers aan BREIN. Dit hoofdstuk gaat in op de vereisten die volgen uit de wet- en regelgeving en een standaardarrest. Hiernaast is de privacywetgeving bekeken.

Hoofdstuk 3 richt zich op de relevante wet- en regelgeving en literatuur omtrent de status van het Lycos/Pessers-arrest.[[37]](#footnote-37) Dit hoofdstuk gaat in op de gebeurtenissen na het standaardarrest. Veel mensen dachten hierdoor dat er een einde aan het Lycos/Pessers-tijdperk was gekomen.[[38]](#footnote-38)

Vervolgens wordt in Hoofdstuk 4 de focus gelegd op de resultaten van het jurisprudentieonderzoek. In dit hoofdstuk worden de overwegingen en beoordelingen van de rechter uit de onderzochte uitspraken middels een aantal onderwerpen geanalyseerd en uiteengezet.

Ten slotte worden in Hoofdstuk 5 de conclusies van de onderzoeksresultaten beschreven. Deze conclusies beogen antwoord te geven op de centrale vraag van dit onderzoek. Deze conclusies leiden tot verschillende aanbevelingen, die worden besproken in Hoofdstuk 6.

# Juridisch kader

In dit hoofdstuk wordt antwoord gegeven op de eerste deelvraag. Deze luidt: ‘In welke gevallen kan BREIN naw-gegevens opvragen, blijkens wet- en regelgeving en literatuuronderzoek?’ Aan bod komen onder andere de onrechtmatige daad, de handhavingsmogelijkheid van de Aw, de vier criteria die voortvloeien uit de rechtspraak, en de privacywetgeving.

## 2.1 Stichting BREIN

BREIN is een stichting met als doel de collectieve bestrijding van auteursrechtinbreuken. BREIN heeft in de afgelopen jaren veelvuldig in rechte opgetreden tegen het ongeautoriseerd aanbieden van entertainmentcontent op internet, met name ten behoeve van haar aangesloten rechthebbenden. De aangeslotenen van BREIN bestaan uit makers inclusief uitvoerende kunstenaars enerzijds en producenten, uitgevers en distributeurs anderzijds. De Nederlandse en internationale (leden van de) aangeslotenen van BREIN vertegenwoordigen tezamen het leeuwendeel van de rechten die er wereldwijd op commercieel beschikbare entertainmentcontent bestaan en op de Nederlandse markt beschikbaar zijn.[[39]](#footnote-39) Dit zijn rechthebbenden in de zin van artt. 12 en 13 Aw.

De statuten van BREIN vermelden de volgende doelstelling: ‘*Het bestrijden van de onrechtmatige exploitatie van informatiedragers en informatie en het te dien einde behartigen van de belangen van de rechthebbenden op informatie en van de rechtmatige exploitanten daarvan, met name van haar aangeslotenen, in het bijzonder door het handhaven, het bevorderen en het verkrijgen van een afdoende juridische bescherming van de rechten en belangen van die rechthebbenden en exploitanten, alles in de ruimste zin.’* BREIN is volgens haar statuten en in samenhang met art. 3:305a BW bevoegd rechtsvorderingen in te stellen ten behoeve van haar aangeslotenen en hun leden. Art. 3:305a lid 1 BW staat een stichting met volledige rechtsbevoegdheid toe om ter bescherming van gelijksoortige belangen van andere personen een rechtsvordering in te stellen, voor zover de stichting deze belangen op grond van haar statuten behartigt.[[40]](#footnote-40) Op grond van haar statuten behartigt BREIN immers de belangen waarvoor zij in een procedure bescherming inroept en deze belangen worden door BREIN ook voldoende gewaarborgd.

Praktisch alle rechthebbenden van de entertainmentcontent die commercieel beschikbaar is, zijn direct of via brancheorganisaties aangesloten bij BREIN. Op basis van art. 3:305a lid 6 BW kan de rechter een rechtspersoon als bedoeld in lid 1 van hetzelfde artikel ontvankelijk verklaren zonder dat de rechtspersoon hoeft te voldoen aan de leden 2 en 5 van art. 3:305a BW. Dit is mogelijk wanneer de rechtsvordering wordt ingesteld met een ideëel doel en een beperkt financieel belang of wanneer de aard van de vordering van de rechtspersoon als bedoeld in lid 1 of van de personen tot bescherming van wier belangen de rechtsvordering strekt, daartoe aanleiding geeft. Bij toepassing van lid 6 kan de rechtsvordering niet strekken tot schadevergoeding in geld. In een procedure tegen een provider tot afgifte van naw-gegevens van een inbreukmaker, beoogt BREIN met name een ideëel doel. Namelijk het bestrijden van inbreuk op de auteursrechten van hun rechthebbenden. BREIN moet verder voldoen aan de aanvullende ontvankelijkheidsvereisten zoals uiteengezet in art. 3:305a lid 3 BW. BREIN voldoet aan de eis die volgt uit lid 1. De bestuurders die betrokken waren bij de oprichting van BREIN noch hun opvolgers hebben een rechtstreeks of middellijk winstoogmerk bij de stichting. Verder moeten vorderingen volgens lid 2 een nauwe band hebben met de Nederlandse rechtssfeer.

## 2.2 Providers

Bij het vorderen van naw-gegevens na inbreuk op auteursrechten op internet zijn de usenet-, access- en hostingproviders de tegenpartij. Het risico bestaat dat klanten de diensten van personen die de toegang tot en het gebruik van internet gebruiken om inbreuk te plegen op de auteursrechten inbreuk van rechthebbenden. De provider is vaak degene die de inbreuk kan stoppen. Op het moment dat de provider weet dat een afnemer van zijn diensten gebruikmaakt voor auteursrechteninbreuk, moet hij maatregelen nemen om die inbreuk te beëindigen.[[41]](#footnote-41)

### 2.2.1 Tussenpersoon

De verschillende providers zijn tussenpersonen. De Organisatie voor Economische Samenwerking en Ontwikkeling (hierna: OESO) geeft als definitie van online-tussenpersonen: “Online-tussenpersonen bundelen of vergemakkelijken transacties tussen derden op internet. Zij geven toegang tot, hosten, verzenden en indexeren inhoud, producten en diensten die afkomstig zijn van derden op internet of bieden ‘Internet-based’ diensten aan derden.”[[42]](#footnote-42)

In geval van onrechtmatige informatie is echter niet de tussenpersoon de primaire inbreukmaker, maar degene die het initiatief neemt en deze laatste persoon kan als zodanig worden aangesproken. Artt. 12-14 e-Commercerichtlijn zien daarom op de vrijstelling van aansprakelijkheid van online-dienstverleners. In de Nederlandse wetgeving zijn deze artikelen geïmplementeerd in art. 6:196c BW.[[43]](#footnote-43) Art. 6:196c lid 4 BW en art. 14 e-Commercerichtlijn zien op de tussenpersonen die in dit onderzoek van belang zijn. Deze artikelen vrijwaren onder bepaalde voorwaarden de providers van de aansprakelijkheid ten opzichte van degene die de op het auteursrecht inbreukmakende content schade heeft geleden.

De eerste voorwaarde is dat de provider geen actieve rol mag hebben gespeeld waardoor hij kennis of controle heeft over de opgeslagen gegevens.[[44]](#footnote-44) Het is van belang dat de provider een neutrale positie inneemt tussen aan de ene kant de rechthebbende van het werk waarop auteursrechtinbreuk is gepleegd en aan de andere kant de klant van die provider.[[45]](#footnote-45) De tweede voorwaarde is dat de tussenpersoon in de eerste plaats niet wist dat de van een ander afkomstige informatie een onrechtmatig karakter heeft. Wanneer een civielrechtelijke procedure gaat over schadevergoeding, mag de provider niet bekend zijn met feiten of omstandigheden op grond waarvan hij redelijkerwijs behoort te weten dat de informatie een onrechtmatig karakter heeft. De provider hoeft in twee gevallen niet aan de onrechtmatigheid te twijfelen. In het eerste geval heeft de rechter de onrechtmatigheid vastgesteld. In het tweede geval is de informatie onmiskenbaar onrechtmatig.[[46]](#footnote-46)

De laatste voorwaarde is dat de tussenpersoon de toegang onmogelijk maakt of de informatie verwijdert wanneer hij op de hoogte wordt gesteld van de onrechtmatigheid.[[47]](#footnote-47) Een voorbeeld hiervan is het voldoen aan een ‘notice-and-take-down’-verzoek. Hierbij wordt de provider op de hoogte gesteld door een rechthebbende dat zijn werk op een website is te vinden. De provider kan dit werk daarna verwijderen. In 2008 is de gedragscode Notice-and-Take-Down opgesteld vanuit de wens van de overheid en marktpartijen om te komen tot afspraken rondom de notice-and-take-down-procedure. De code heeft als doel partijen te helpen om binnen de bestaande wettelijke kaders zorgvuldig te opereren bij het verwijderen van informatie van internet, op verzoek van derden. Hierbij kan worden gedacht aan een rechthebbende wiens werk openbaar is gemaakt. De code richt zich daarom op de afhandeling van meldingen ten aanzien van de (vermeende) onrechtmatige ‘en’ of ‘of’ strafbare informatie op internet. Hierbij is het streven dat private partijen dit soort meldingen zo veel mogelijk zelf afhandelen. Eveneens kan de gedragscode worden gebruikt voor de eventuele inhoud die door een tussenpersoon zelf als ongewenst of schadelijk wordt aangemerkt.[[48]](#footnote-48)

Op grond van art. 8 lid 3 van de Auteursrechtrichtlijn en art. 11 van de Handhavingsrichtlijn moeten de lidstaten voorzien in de mogelijkheid van een gerechtelijk bevel tegen tussenpersonen die door derden voor inbreukdoeleinden worden gebruikt. Dit is geïmplementeerd in art. 6:196c lid 5 BW.[[49]](#footnote-49) De vrijwaring van aansprakelijkheid van de provider sluit volgens art. 6:196c lid 5 BW een rechterlijk verbod of gebod niet uit. Een tussenpersoon kan via een rechterlijk bevel worden bevolen om de auteursrechtinbreuk te staken of te verwijderen. Hieraan kan een dwangsom worden verbonden.

## 2.3 Auteursrecht

Zoals beschreven in Paragraaf 2.1 heeft BREIN als doel de collectieve bestrijding van auteursrechtinbreuken. Die inbreuk bestaat er in dit geval uit dat een derde de diensten van een provider gebruikt om illegale content te plaatsen. Het auteursrecht is een onderdeel van het intellectueel-eigendomsrecht.[[50]](#footnote-50) Grotendeels is het te vinden in bijzondere wetten en internationale regelgeving, zoals de eerder genoemde Handhavingsrichtlijn en Auteursrechtrichtlijn. Het auteursrecht is nationaal geregeld in de Aw. In 1954 was er een opzet voor een nieuw BW, waarin onder andere het auteursrecht in boek 9 werd ondergebracht. Het ontwerp van boek 9 heeft niet geleidt tot wijziging van het BW. Dit kwam mede door de aanzienlijke hoeveelheid niet-privaatrechtelijke regels in de intellectueel-eigendomswetgeving.[[51]](#footnote-51) In 1994 heeft het Ministerie van Justitie gekeken naar de mogelijkheid van boek 9. Hier kwam ook dezelfde conclusie uit. De meeste deelgebieden van het intellectuele eigendomsrecht door verdragen en Europese richtlijnen wordt beheerst.[[52]](#footnote-52)

Het auteursrecht is ontstaan om de maker van een werk de mogelijkheid te geven zijn werk te exploiteren en hem bescherming te bieden voor de integriteit van zijn geestelijke schepping.[[53]](#footnote-53) Volgens art. 1 Aw is het auteursrecht het “uitsluitend recht van de maker van een werk van letterkunde, wetenschap of kunst, of diens rechtverkrijgenden, om dit openbaar te maken en te verveelvoudigen, behoudens de beperkingen, bij de wet gesteld”. Auteursrecht is een uitsluitend recht, omdat het de uitsluitende bevoegdheid geeft het werk openbaar te maken en te verveelvoudigen.[[54]](#footnote-54) De inbreukmaker die het werk van de auteursrechthebbende online plaatst, maakt het werk openbaar en verveelvoudigt het werk. De rechthebbende heeft hiervoor geen toestemming gegeven en daardoor wordt inbreuk gemaakt op de auteursrechten van de rechthebbende. BREIN kan hierdoor tegen deze inbreuken optreden.

Het auteursrecht is vergelijkbaar met het eigendomsrecht. Bij overdracht van het eigendom, oftewel het werk, verleent de rechthebbende toestemming om het werk te tonen bijvoorbeeld, veelal op bepaalde financiële voorwaarden. Het auteursrecht beschermt een werk tegen exploitatie zowel in de vorm waarin het gemaakt is als in bewerking of vertaling, en beschermt tegen zowel gehele als gedeeltelijke overname.[[55]](#footnote-55) Het auteursrecht verleent de auteursrechten met betrekking tot tal van vormen van gebruik van de rechthebbende zijn werk. Voor een groot aantal handelingen is de toestemming van de rechthebbende nodig. De Aw vat deze handelingen samen in de termen ‘openbaar maken’ en ‘verveelvoudigen’.

### 2.3.1 Openbaar maken

Onder de term ‘openbaar maken’ vat de Aw een aantal handelingen samen die met elkaar gemeen hebben dat het werk op de een of andere manier ter beschikking van een publiek wordt gesteld.[[56]](#footnote-56) Deze handelingen zijn opgesomd in art. 12 lid 1 Aw. Hierbij wordt onderscheid gemaakt tussen materiële en immateriële openbaarmaking. Materiële openbaarmaking vindt plaats door het in het verkeer brengen van het stoffelijk voorwerp waarin het werk is vastgelegd, zoals het uitgeven van een boek of dvd. Immateriële openbaarmaking is het uitvoeren van een toneelstuk, of het uitzenden of het via internet ter beschikking stellen van een film.[[57]](#footnote-57)

Bij verdere openbaarmaking wordt het ingewikkelder, omdat het werk dan door een derde opnieuw wordt gebruikt.[[58]](#footnote-58) Een voorbeeld hiervan is een radiozender die verschillende muziekwerken speelt. Als een caféhouder deze zender afspeelt in zijn café, dan maakt hij de muziekwerken ook openbaar. In dit geval is de derde de caféhouder.[[59]](#footnote-59) Een moderner voorbeeld is een YouTube-video waarin op de achtergrondmuziek te horen is. De muziek staat in deze video niet centraal.

De in dit onderzoek relevante inbreukmaker maakt gebruik van immateriële openbaarmaking. De uploader maakt de content openbaar via usenet of BitTorrent. Hij plaatst alleen de film online op de illegale website. De verdere openbaarmaking is niet van toepassing op de uploader, die centraal staat in deze afstudeeropdracht.

### 2.3.2 Verveelvoudigen

Volgens art. 13 Aw wordt onder de verveelvoudiging van een werk van letterkunde, wetenschap of kunst mede verstaan “de vertaling, de muziekschikking, de verfilming of toneelbewerking en in het algemeen iedere gehele of gedeeltelijke bewerking of nabootsing in gewijzigde vorm, welke niet als een nieuw, oorspronkelijk werk moet worden aangemerkt”. De term ‘verveelvoudigen’ wordt gebruikt in twee verschillende betekenissen.[[60]](#footnote-60) Enerzijds is dit het vervaardigen van exemplaren waarin het werk is vastgesteld.[[61]](#footnote-61) De inbreng van degene die verveelvoudigt, heeft geen betekenis; hij schept immers niets. De inbreukmaker kenmerkt zich veelal doordat hij zijn eigen inbreng verdoezelt.[[62]](#footnote-62) Anderzijds is verveelvoudigen het bewerken of nabootsen van het werk in gewijzigde vorm.[[63]](#footnote-63) Hier gaat het niet om een exacte kopie, maar om afgeleiden van het oorspronkelijke werk. Beslissend is of de bewerker auteursrechtelijk beschermde trekken van het oorspronkelijke werk herkenbaar overneemt.[[64]](#footnote-64) Enkele voorbeelden zijn het ondertitelen van een film en een verfilming van een boek.[[65]](#footnote-65)

Een uploader kan voldoen aan beide betekenissen. Hij kan materiaal plaatsen dat hij kopieert van een dvd of van een opname van televisieserie. De uploader kan ook een tijdschrift of e-book delen. Bij de andere betekenis van verveelvoudigen plaatst de uploader films of televisieseries op internet waaraan hij zelf een ondertiteling heeft toegevoegd.[[66]](#footnote-66)

### 2.3.3 Ontwikkelingen

In de afgelopen decennia is de technologische ontwikkeling sterk toegenomen. Met name auteursrechtelijk beschermde muziek en films worden veelvuldig digitaal uitgewisseld.[[67]](#footnote-67) Tegenwoordig wordt via internet op grote schaal inbreuk gemaakt op het intellectueel-eigendomsrecht.[[68]](#footnote-68) De begrippen ‘werk’, ‘openbaar maken’ en verveelvoudigen’ hebben een ‘open’ en technologieonafhankelijk karakter. Hierdoor kunnen de ontwikkelingen door de rechter en wetgever relatief eenvoudig in het auteursrechtelijke systeem geïntegreerd worden.[[69]](#footnote-69) [[70]](#footnote-70) Dit betekent echter niet dat de ontwikkelingen steeds harmonisch zijn verlopen. Ze hebben niet alleen geleid tot nieuwe mogelijkheden, maar ook tot aanzienlijke verschuivingen. Enerzijds zijn de rechten van de rechthebbende verruimd.[[71]](#footnote-71) Aan de andere kant staat dat de gebruikers meer in staat zijn om kopieën van de werken te maken.[[72]](#footnote-72)

## 2.4 Handhaving

In Paragraaf 2.2.1 is de Handhavingsrichtlijn genoemd. Het doel van deze Handhavingsrichtlijn is “een hoog, gelijkwaardig en homogeen niveau van bescherming in de interne markt te waarborgen”.[[73]](#footnote-73) [[74]](#footnote-74) In overwegingen 1, 2 en 3 wordt daartoe vooropgesteld dat een doeltreffende handhaving van intellectueel-eigendomsrechten, en daarmee van het eerder beschreven auteursrecht, van essentieel belang is. Dit ter bescherming van de mogelijkheid van rechthebbenden om inkomsten met hun werk te genereren en ter bevordering van innovatie, creativiteit en een zo groot mogelijke verspreiding van werken, denkbeelden en kennis. “Zonder doeltreffende middelen om intellectueel-eigendomsrechten te handhaven, worden innovatie en creativiteit echter ontmoedigd en investeringen verminderd”, aldus overweging 3 van de richtlijn. In lijn daarmee bepaalt art. 3 lid 2 Handhavingsrichtlijn dat de ter uitvoering van de richtlijn vastgestelde maatregelen, procedures en rechtsmiddelen “doeltreffend, evenredig en afschrikkend” moeten zijn.

Voor een doeltreffende handhaving van intellectueel-eigendomsrechten is het vanzelfsprekend een noodzakelijke voorwaarde dat de rechthebbende weet wie de inbreukmaker is, zodat deze aangesproken kan worden en nieuwe inbreuken voorkomen kunnen worden. De Handhavingsrichtlijn voorziet daartoe in een “recht op informatie waardoor waardevolle gegevens kunnen worden verkregen over de herkomst van de inbreukmakende goederen of diensten, de distributiekanalen en de identiteit van bij de inbreuk betrokken derden”.[[75]](#footnote-75) Dit recht is uitgewerkt in art. 8 van de richtlijn. Dit artikel bepaalt onder het kopje ‘Recht op informatie’ (onder meer) dat derden die op commerciële schaal diensten verlenen die bij inbreukmakende handelingen worden gebruikt, gelast kunnen worden informatie te verstrekken over “de herkomst en de distributiekanalen van de goederen of diensten” (lid 1), waaronder “de naam en het adres van de producenten, fabrikanten, distributeurs, leveranciers en andere eerdere bezitters van de goederen of diensten” (lid 2, onder a).

Bij de toepassing van art. 8 van de Handhavingsrichtlijn dient daarom een afweging plaats te vinden tussen twee botsende grondrechten die door het Handvest worden erkend: het recht op bescherming van persoonsgegevens (art. 8 Handvest) en het recht op bescherming van intellectueel eigendom (art. 17 lid 2 Handvest). Deze grondrechten worden verder besproken in Paragraaf 2.9. Het Handvest is relevant, omdat het steeds meer invloed heeft op het recht van intellectueel eigendom.[[76]](#footnote-76)

De Handhavingsrichtlijn bevat minimale eisen waaraan lidstaten moeten voldoen. De lidstaten moeten er daarom voor zorgen dat hun wet- en regelgeving aan de Handhavingsrichtlijn voldoet. In een procedure kan een partij geen rechtstreeks beroep doen op de Handhavingsrichtlijn.[[77]](#footnote-77) Art. 8 van de Handhavingsrichtlijn is in Nederland onder andere geïmplementeerd in art. 1019f Rv, art. 28 lid 9 Aw, art. 17 lid 6 Wet op de naburige rechten, art. 5c lid 5 Databankenwet en art. 70 lid 10 Rijksoctrooiwet 1995, alsmede in art. 2.22 lid 4 en lid 5 van het Benelux-verdrag inzake de intellectuele eigendom. Deze regels vervangen de oudere regelgeving, al is de open norm van de onrechtmatige daad blijven bestaan.

De Handhavingsrichtlijn biedt een aantal nieuwe middelen om auteursrechten te handhaven. Een van de handhavingsmogelijkheden is het recht op informatie. BREIN kan op drie manieren naw-gegevens bemachtigen. Een daarvan is via het strafrecht; de andere twee lopen via het civiele recht. Hierbij kan BREIN naw-gegevens vorderen via een rechterlijk bevel op grond van art. 28 lid 9 Aw of via art. 6:162 lid 2 BW in combinatie met het Lycos/Pessers-arrest.[[78]](#footnote-78)

## 2.5 Strafrechtelijke vervolging

Een van de drie mogelijkheden om naw-gegevens te bemachtigen, is via strafrechtelijke vervolging. Op basis van de Aw is inbreuk op auteursrecht strafbaar gesteld; dit staat in art. 31 Aw, jo. art. 31a Aw. Volgens art. 31 Aw is iemand die opzettelijk inbreuk maakt op het auteursrecht van een ander, strafbaar. De straf hierop is een gevangenisstraf van ten hoogste zes maanden of een geldboete van de vierde categorie. Aangezien de wetgever echter aanstuurt op civielrechtelijke handhaving, heeft bestrijding van inbreuk geen prioriteit bij het Openbaar Ministerie.[[79]](#footnote-79) Het is in eerste instantie een taak van de rechthebbende zelf om zijn intellectueel-eigendomsrechten te handhaven via de civielrechtelijke weg. Dit blijkt met name uit de aanwijzing intellectueel-eigendomsfraude die nog steeds aangehaald wordt in rechtszaken, hoewel deze aanwijzing vervallen is op 1 april 2017.[[80]](#footnote-80)

Op grond van art. 54a Wetboek van Strafrecht is de neutrale tussenpersoon in beginsel strafrechtelijk gezien niet aansprakelijk. Art. 54a Wetboek van Strafrecht is het strafrechtelijke evenbeeld van art. 6:196c BW.[[81]](#footnote-81) Er zijn weinig zaken bekend waarin de strafrechtelijke aansprakelijkheid van een tussenpersoon aan de orde was.[[82]](#footnote-82) Daarom is in dit onderzoek de strafrechtelijke aansprakelijkheid van de tussenpersoon buiten beschouwing gelaten.

## 2.6 Rechterlijk bevel

De handhaving van auteursrechten is primair een civielrechtelijke aangelegenheid, zoals uit de vorige paragraaf is gebleken.[[83]](#footnote-83) Uit de inleiding van dit hoofdstuk is gebleken dat er twee civielrechtelijke mogelijkheden zijn om naw-gegevens te verkrijgen. De eerste relevante mogelijkheid is te vinden in art. 28 lid 9 Aw. Voor de benadeelde, in de hoedanigheid van rechthebbende, is de tweede zin van art. 28 lid 9 Aw relevant: *‘Onder dezelfde voorwaarden kan dit bevel worden gegeven aan een derde die op commerciële schaal inbreukmakende goederen in zijn bezit heeft of gebruikt, die op commerciële schaal diensten verleent die bij de inbreuk worden gebruikt, of die door een van deze derden is aangewezen als zijnde betrokken bij de productie, fabricage of distributie van deze goederen of bij het verlenen van deze diensten.’*

De zin is gericht op een ‘bevel aan een derde’, oftewel een tussenpersoon. De provider is de relevante tussenpersoon in dit onderzoek. De provider valt onder de categorie derde “die op commerciële schaal diensten verleent die bij de inbreuk worden gebruikt”.[[84]](#footnote-84) In dit artikel kan een tussenpersoon een bevel krijgen om de naw-gegevens af te geven. Uit de parlementaire geschiedenis blijkt dat hieronder ook de naw-gegevens en het IP-adres worden verstaan.[[85]](#footnote-85) Dit bevel zal echter wel ‘op vordering van de gerechtigde’ moeten worden gedaan. De benadeelde is ten aanzien van het auteursrecht daarom genoodzaakt een gerechtelijke procedure te starten teneinde de naw-gegevens en het IP-adres van de (mogelijke) dader te achterhalen. Volgens art. 28 lid 9 Aw moet BREIN altijd naar de rechter om naw-gegevens van de provider te verkrijgen.

## 2.7 Onrechtmatige daad

De andere civielrechtelijke mogelijkheid voor afgifte is de onrechtmatige daad. Onder het woord ‘daad’ wordt niet alleen een doen verstaan, maar ook een nalaten.[[86]](#footnote-86) De onrechtmatige daad is vastgelegd in art. 6:162 BW. Art. 6:162 lid 2 BW omschrijft drie gronden waarop een bepaalde gedraging als onrechtmatige daad kan worden aangemerkt. Dit zijn een inbreuk op een recht, een doen of nalaten in strijd met een wettelijke plicht, en een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt.[[87]](#footnote-87)

Bij een inbreuk op een recht moet het gaan om een inbreuk op subjectieve rechten. Hierbij worden twee soorten subjectieve rechten onderscheiden: de absolute vermogensrechten en de persoonlijkheidsrechten.[[88]](#footnote-88) Volgens art. 3:6 BW zijn intellectueel-eigendomsrechten absolute vermogensrechten op niet-materiële objecten.[[89]](#footnote-89) Absolute rechten gelden ten opzichte van iedereen en de rechthebbende kan bepalen wat hij met het goed doet.[[90]](#footnote-90)

BREIN vordert meestal naw-gegevens van de provider op basis van de onrechtmatige daad. Een belangrijke consequentie van art. 6:162 lid 1 BW is dat de dader van een onrechtmatige daad verplicht kan worden de door zijn gedraging aan een ander toegebrachte schade te vergoeden.[[91]](#footnote-91)

## 2.8 Lycos/Pessers-arrest

De civielrechtelijke mogelijkheid tot afgifte van naw-gegevens via de onrechtmatige daad, wordt gebruikt in combinatie met het Lycos/Pessers-arrest.[[92]](#footnote-92) Dit bevat een belangrijke uitspraak als het gaat om de afgifte van naw-gegevens. Pessers, een postzegelhandelaar die via de website ebay.com in postzegels handelde, werd op een door Lycos gehoste website beschuldigd van onder meer oplichting. In kort geding vorderde Pessers dat Lycos de naw-gegevens van de websitehouder aan hem bekend zou maken. Dit arrest uit 2005 wordt gebruikt door rechters om het vraagstuk over afgifte van naw-gegevens te beoordelen. De Hoge Raad heeft in dit arrest bepaald dat onder bepaalde omstandigheden de rechtsplicht tot afgifte van de naw-gegevens aan een derde kan bestaan. Hierbij heeft de Hoge Raad vier criteria vastgesteld voor de afgifte van naw-gegevens door isp’s (later is dit uitgebreid naar andere tussenpersonen[[93]](#footnote-93)). De vier criteria zijn:

1. “de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk;
2. de derde heeft een reëel belang bij de verkrijging van de naw-gegevens;
3. aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de naw-gegevens te achterhalen;
4. afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren”.[[94]](#footnote-94)

De Hoge Raad oordeelde dat het Gerechtshof of het belang van Pessers bij de verkrijging van de persoonsgegevens op de juiste wijze had afgewogen tegen het recht op eerbiediging van de persoonlijke levenssfeer. Verder oordeelde de Hoge Raad dat de destijds geldende Wet bescherming persoonsgegevens de verstrekking van de naw-gegevens niet in de weg stond, omdat Pessers een gerechtvaardigd belang had in de zin van art. 8 sub f Wet bescherming persoonsgegevens.[[95]](#footnote-95) Dit artikel is vrijwel identiek aan art. 6 sub f AVG,[[96]](#footnote-96) al legt het laatste artikel extra nadruk op de eventuele zwaarder wegende “belangen of de grondrechten en de fundamentele vrijheden” van het kind.

Tussenpersonen kunnen op grond van het Lycos/Pessers-arrest geen absoluut weigeringsbeleid voeren. Als aan de criteria is voldaan, maar de tussenpersoon blijft weigeren naw-gegevens af te staan, kan ook de tussenpersoon door de belanghebbende aansprakelijk gesteld worden voor zijn onrechtmatig handelen. [[97]](#footnote-97)

## 2.9 Belangenafweging

Het vierde criterium, de belangenafweging, is het lastigste criterium.[[98]](#footnote-98) De belangrijkste grondrechten die hierbij tegenover elkaar staan, zijn het recht op bescherming van eigendom en het recht op bescherming van persoonsgegevens.[[99]](#footnote-99)

Het eerste belangrijke grondrecht is het recht op bescherming van eigendom, met inbegrip van intellectueel eigendom. Dit grondrecht is beschreven is in art. 17 lid 2 Handvest. Hoewel dit recht in het Handvest in absolute termen is vervat (“Intellectuele eigendom is beschermd”), overweegt het Hof van Justitie dat “noch uit deze bepaling, noch uit de rechtspraak van het Hof [voortvloeit] dat dit recht onaantastbaar is en daarom absolute bescherming moet genieten”.[[100]](#footnote-100) Art. 52 lid 1 Handvest laat de lidstaten vrij de in het Handvest gewaarborgde grondrechten bij wet te beperken, mits de kern ervan niet wordt aangetast en met inachtneming van het evenredigheidsbeginsel. In casu zal de handhaving van het auteursrecht moeten worden afgewogen tegen andere in het Handvest gewaarborgde grondrechten; er zal een “juist evenwicht” (‘fair balance’) tussen deze rechten gevonden moeten worden.[[101]](#footnote-101)

Het tweede belangrijke grondrecht, het recht op bescherming van persoonsgegevens, is beschreven in art. 8 Handvest. Dit recht houdt in dat elk individu het recht heeft dat zijn persoonsgegevens op een rechtmatige wijze worden verwerkt, om te voorkomen dat hij hier nadeel van ondervindt.[[102]](#footnote-102)

Naast deze twee belangrijke grondrechten zijn er andere grondrechten die de rechter betrekt in de belangenafweging. Deze grondrechten vloeien voort uit het Scarlet Extended/SABAM-arrest en dan met name de conclusie van advocaat-generaal Cruz Villalón.[[103]](#footnote-103) [[104]](#footnote-104) Hij weegt de grondrechten privacy en communicatiegeheim (art. 7 Handvest), persoonsgegevens (art. 8 Handvest) en informatievrijheid (art. 11 Handvest) af tegen het recht op bescherming van eigendom. De grondrechtelijke toetsing door het Hof van Justitie verloopt echter anders. Het Hof van Justitie stelt de vrijheid van ondernemerschapvan art. 16 Handvest voorop.[[105]](#footnote-105) In het Scarlet Extended/SABAM-arrest stelt het Hof van Justitie dat het auteursrecht geen voorrang heeft op andere grondrechten, maar dat het in geval van conflict op gelijke voet moet worden afgewogen met andere fundamentele rechten.[[106]](#footnote-106)

Art. 7 Handvest gaat over de eerbiediging van het privéleven en van het familie- en gezinsleven. Het artikel luidt: “Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.” Dit artikel komt overeen met de rechten die vermeld staan in art. 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). Dit fundamentele recht maakt samen met art. 8 Handvest deel uit van het recht op privacy.[[107]](#footnote-107) He Nederlandse equivalent hiervan is art. 10 Grondwet. In dit artikel wordt bepaald dat eenieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer.

Art. 11 Handvest gaat in op de vrijheid van meningsuiting en de informatievrijheid. Art. 11 lid 1 luidt: “Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.” Dit artikel komt overeen met de rechten die vermeld staan in art. 10 EVRM.

Vrijheid van ondernemerschap vloeit voort uit art. 16 Handvest. Volgens het Hof van Justitie in het Scarlet Extended/SABAM-arrest zou een gerechtelijk filtergebod de internetproviders op hoge kosten jagen en daardoor leiden tot “een ernstige beperking van de vrijheid van ondernemerschap van de betrokken internetprovider”.[[108]](#footnote-108) Dit komt door de technisch ingrijpende maatregel, de geldingsduur en de kosten (verdeling van de maatregel). Hierdoor zou geen “juist evenwicht” worden bereikt tussen de bescherming van het intellectueel eigendomsrecht en de vrijheid van ondernemerschap.[[109]](#footnote-109)

2.10 Algemene verordening gegevensbescherming

Uit de vorige paragraaf blijkt dat de privacy van de inbreukmaker een belangrijke rol speelt bij afgifte van naw-gegevens. Om de persoonsgegevens te beschermen, geldt sinds 25 mei 2018 in de EU nieuwe regelgeving over de verwerking van naw-gegevens; dit is de AVG. Deze bescherming was voorheen uitgewerkt in de Databeschermingsrichtlijn.[[110]](#footnote-110) In Nederland was de Wet bescherming persoonsgegevens gebaseerd op de Databeschermingsrichtlijn.[[111]](#footnote-111) Nederland heeft ter uitvoering van de AVG de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG) opgesteld.[[112]](#footnote-112) De AVG en de UAVG moeten in samenhang worden gelezen.[[113]](#footnote-113)

Door snelle technologische ontwikkelingen en globalisering zag de EU zich geconfronteerd met nieuwe uitdagingen om persoonsgegevens te kunnen beschermen. Die ontwikkelingen vereisten volgens de EU een krachtig en coherent kader voor gegevensbescherming, dat wordt gesteund door strenge handhaving.[[114]](#footnote-114) De vijf belangrijkste redenen voor de ontwikkeling van de AVG zijn: harmonisering van de regels, harmonisering van de handhaving, versterking van de handhaving, democratisering van de handhaving, en bewustwording.[[115]](#footnote-115) De AVG heeft als doel, volgens art. 1 AVG, de regulatie van de omgang met persoonsgegevens, oftewel de verwerking van persoonsgegevens.[[116]](#footnote-116)

De AVG geeft iets meer invulling van en aanvulling op de bescherming van de privacy van personen dan de vorige richtlijn.[[117]](#footnote-117) Voor de verwerking van persoonsgegevens gelden nu meer en strengere regels. Enerzijds zijn de privacyrechten van de betrokkene versterkt en uitgebreid, anderzijds hebben tussenpersonen meer verantwoordelijkheden gekregen.[[118]](#footnote-118) De betrokkene is degene van wie de persoonsgegevens worden verwerkt, volgens art. 4 lid 1 AVG.

De AVG kent verschillende beginselen van gegevensbescherming, die terug te vinden zijn in art. 5 lid 1 AVG. Bij elke verwerking van persoonsgegevens dienen de volgende beginselen in acht te worden genomen: rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit en vertrouwelijkheid.[[119]](#footnote-119) Deze basisbeginselen hebben zelfstandige betekenis als norm.[[120]](#footnote-120) Een betrokkene kan zich hier rechtstreeks op beroepen bij de rechter of toezichthouder om bijvoorbeeld een belangenafweging anders te laten uitvallen of een bepaalde verwerking te doen staken.[[121]](#footnote-121)

### 2.10.1 Rechtmatigheid van verwerking

Een van de beginselen van de AVG is dat persoonsgegevens rechtmatig moeten worden verwerkt, oftewel: het doel voor de verwerking moet rechtvaardig zijn. Dit volgt uit art. 5 lid 1 sub a AVG. De gegevensverwerking is gerechtvaardigd indien het doel van de verwerking kan worden gebaseerd op een van de zes grondslagen van art. 6 AVG. Deze grondslagen zijn: toestemming, overeenkomst, wettelijke verplichting, noodzakelijk om de vitale belangen te beschermen, noodzakelijk voor een taak in het algemeen belang, en gerechtvaardigd belang. De grondslagen zijn limitatief. Het aanvoeren van een andere rechtsgrond is daarom niet mogelijk. Verder zijn de grondslagen niet cumulatief: om de gegevensverwerking te rechtvaardigen, hoeft slechts aan een van de grondslagen te zijn voldaan.[[122]](#footnote-122)

In het kader van het vraagstuk van deze afstudeeropdracht is de verwerking van de persoonsgegevens noodzakelijk voor de behartiging van gerechtvaardigde belangen. Het gerechtvaardigde belang van BREIN is de inbreukmaker in rechte te kunnen betrekken, zodat de inbreuk op de rechten van haar rechthebbende stopt. Deze grondslag kan alleen gebruikt worden volgens art. 6 sub f AVG als de belangen of grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke.[[123]](#footnote-123) Indien het recht op privacy prevaleert, mogen tussenpersonen de naw-gegevens en het IP-adres van de (mogelijke) inbreukmaker niet afgeven. De vraag is wanneer het recht op privacy van de (mogelijke) dader prevaleert boven het belang van de benadeelde om de inbreukmaker in rechte te kunnen betrekken.

### 2.10.2 Verantwoordingsplicht

Met de komst van de AVG krijgen organisaties een grotere verantwoordelijkheid bij het verwerken van persoonsgegevens, de verantwoordingsplicht. Deze is terug te vinden in art. 5 lid 2 AVG. Art. 24 lid 1 AVG gaat verder in op de verantwoordingsplicht van organisaties. De verwerkingsverantwoordelijke is verplicht passende en effectieve maatregelen te nemen om naleving van de AVG te borgen en moet kunnen aantonen dat elke verwerkingsactiviteit past binnen de AVG.[[124]](#footnote-124)

Vijf concrete stappen die een organisatie moet nemen, zijn:

* documenteren;
* een functionaris voor gegevensbescherming aanstellen;
* een effectbeoordeling uitvoeren;
* zorgen voor goede beveiliging van persoonsgegevens;
* transparant zijn.[[125]](#footnote-125)

Daarnaast dienen organisaties de juiste technische en organisatorische maatregelen te nemen voor de bescherming van persoonsgegevens: ‘privacy by design’ en ‘privacy by default’.[[126]](#footnote-126) Privacy by design houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen en de vereisten uit de AVG. Onder privacy by default wordt verstaan dat de standaardinstellingen zo zijn gekozen dat de privacy maximaal wordt gewaarborgd.[[127]](#footnote-127)

De AVG is nu twee jaar actief, maar hoe deze wet samen met de UAVG wordt gebruikt in een zaak over afgifte van naw-gegevens door providers is nog onzeker. Op dit moment zijn er twee rechtszaken geweest.[[128]](#footnote-128) [[129]](#footnote-129) In een andere rechtszaak tegen een tussenpersoon waarin afgifte van de naw-gegevens werd gevorderd, is getoetst of verstrekking van deze gegevens een toereikende grondslag heeft volgens de AVG.[[130]](#footnote-130)

### 2.10.3 Recht van bezwaar

Paragrafen 2.10.3 en 2.10.4 behandelen de verplichtingen van de provider. De onderzoeker heeft ervoor gekozen om deze verplichtingen toe te voegen, omdat door de twee verplichtingen het verzoek tot afgifte van de naw-gegevens bij de provider veel langer kan duren.

De (mogelijke) inbreukmaker heeft de mogelijkheid op grond van de AVG bezwaar te maken tegen de verwerking van zijn naw-gegevens. Hij heeft met art. 21 AVG het recht van bezwaar, doordat de verwerking plaatsvindt op grond van art. 6 lid 1 sub f AVG. Bij deze grondslag hoort een belangenafweging. De betrokkene kan in een specifieke situatie anders tegen deze afweging aankijken. Hij krijgt de mogelijkheid met het recht van bezwaar om van de verwerkingsverantwoordelijke te verlangen dat deze de afweging nogmaals maakt met de specifieke situatie in het achterhoofd.[[131]](#footnote-131) Volgens art. 21 lid 4 AVG moet de verwerkingsverantwoordelijke, in dit geval de provider, uiterlijk op het moment van het eerste contact met de betrokkene dit recht uitdrukkelijk onder de aandacht van de (mogelijke) inbreukmaker brengen. Dit moet volgens hetzelfde lid duidelijk en gescheiden van enige andere informatie worden weergegeven.[[132]](#footnote-132)

Wanneer de (mogelijke) inbreukmaker van dit recht gebruikmaakt, moet de verwerkingsverantwoordelijke, in dit geval de provider, de verwerking van de naw-gegevens staken. De (mogelijke) inbreukmaker beperkt dan de verwerking. Dit is blijkens art. 18 lid 1 sub d AVG in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene. Blijkens art. 12 lid 3 AVG moet de provider, in ieder geval binnen een maand na ontvangst van het verzoek, informatie over het gevolg van het verzoek geven. Indien nodig kan de termijn met nog eens twee maanden worden verlengd, maar dan dient de provider ook binnen een maand kennis te geven van deze verlenging. Wanneer de beslissing is genomen door een bestuursorgaan, geldt deze als een beslissing in de zin van de Algemene wet bestuursrecht volgens art. 34 UAVG.

Wanneer de provider heeft besloten dat de verwerking doorgaat, wordt de (mogelijke) inbreukmaker op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven. Dit is vermeld in art. 18 lid 3 AVG. Volgens art. 12 lid 4 AVG deelt de provider dan ook mee waarom het verzoek zonder gevolg is gebleven. De provider informeert hem tevens over de mogelijkheid een klacht in te dienen bij een toezichthoudende autoriteit, in Nederland de Autoriteit Persoonsgegevens, en beroep bij de rechter in te stellen. Blijkens art. 35 leden 1 en 2 UAVG moet dit beroep schriftelijk worden ingediend binnen zes weken na ontvangst van het antwoord van de provider. Lid 2 vermeldt dat wanneer de provider zich niet heeft gehouden aan de termijn de (mogelijke) inbreukmaker zich ook niet hoeft te houden aan de termijn van zes weken. De rechtbank kan de partijen en anderen verzoeken schriftelijke inlichtingen te geven en de onder hen berustende stukken in te zenden binnen een door haar te bepalen termijn. Dit blijkt uit art. 35 lid 6 UAVG.

Wanneer de (mogelijke) inbreukmaker zich wendt tot de Autoriteit Persoonsgegevens, worden dezelfde termijnen aangehouden, volgens art. 36 lid 1 UAVG. Volgens ditzelfde artikel kan de Autoriteit Persoonsgegevens bemiddelen of adviseren of gebruik kan worden gemaakt van de geschillenbeslechtingsregeling.

Op het recht van bezwaar zijn wel enkele uitzonderingen. Art. 21 lid 1 AVG vermeldt dat de provider niet hoeft te staken indien hij “dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering”. Andere uitzonderingen worden genoemd in art. 41 lid 1 UAVG. Deze komen overeen met de uitzonderingen zoals genoemd in art. 23 lid 1 AVG.

Het proces van het recht van bezwaar kan langdurig zijn, omdat providers liever geen naw-gegevens afgeven. Hierdoor zullen deze tussenpersonen niet snel stellen dat de dwingende gerechtvaardigde gronden zwaarder wegen dan de belangen, rechten en vrijheden van de (mogelijke) inbreukmaker. Het recht van bezwaar kan worden omzeild door een rechtsvordering. Daarnaast geldt het recht van bezwaar alleen wanneer BREIN naw-gegevens verzoekt van de provider door zich te beroepen op de onrechtmatige daad in combinatie met het Lycos/Pessers-arrest.[[133]](#footnote-133)

### 2.10.4 Recht op gegevenswissing

Wanneer er geen prevalerende dwingende gerechtvaardigde gronden van de verwerking zijn, heeft de betrokkene het recht op gegevenswissing. Dit kan hij verkrijgen op grond van art. 17 lid 1 sub c AVG. De provider is dan verplicht de naw-gegevens zonder onredelijke vertraging te wissen, volgens art. 17 lid 1 AVG.

## 2.11 Conclusie

BREIN kan naw-gegevens opvragen voor haar rechthebbende. Hiervoor kan ze zich wenden tot een tussenpersoon, in dit onderzoek een provider, op basis van art. 3:305a BW in combinatie met haar statuten. BREIN kan bij de provider naw-gegevens opvragen van een inbreukmaker die het werk van de auteursrechthebbende openbaar maakt of verveelvoudigt. Om naw-gegevens te kunnen verkrijgen van een provider kan BREIN het beste de civielrechtelijke handhaving kiezen. De eerste mogelijkheid is via art. 28 lid 9 Aw. BREIN moet in dit geval altijd naar de rechter om naw-gegevens van de provider te verkrijgen.

BREIN kan ook naw-gegevens vorderen op basis van art. 6:162 BW, oftewel de onrechtmatige daad, in combinatie met het Lycos/Pessers-arrest.[[134]](#footnote-134) In dit arrest heeft de Hoge Raad vier criteria bepaald. Wanneer aan deze criteria voldaan wordt, moet de provider de naw-gegevens afgeven. Het laatste criterium van het Lycos/Pessers-arrest is een belangenafweging.[[135]](#footnote-135) Hierbij worden de verschillende grondrechten tegen elkaar afgewogen. Bij de belangenafweging weegt het recht op bescherming van eigendom voor BREIN uiteindelijk zwaarder dan de grondrechten van de provider en mogelijke inbreukmaker die voortvloeien uit het Handvest.

Sinds de AVG gelden er meer en strengere regels voor de verwerking van persoonsgegevens. De rechtmatigheid van de verwerking is hierbij relevant. Verder moet BREIN ervoor zorgen dat zij aan haar verantwoordingsplicht voldoet. Hiervoor kan BREIN de volgende stappen nemen: documenteren, een functionaris voor gegevensbescherming aanstellen, een effectbeoordeling uitvoeren, zorgen voor goede beveiliging van persoonsgegevens en transparant zijn. Ook moet BREIN rekening houden met het recht van bezwaar. Dit recht is echter niet geldig wanneer BREIN een rechterlijk bevel heeft. De rechter weegt het recht van de betrokkene mee in zijn overweging.

BREIN kan naw-gegevens opvragen bij providers wanneer een auteursrechtelijke inbreuk is gepleegd op het werk van haar rechthebbende. BREIN moet hierbij rekening houden met de criteria die zijn genoemd in het Lycos/Pessers-arrest.[[136]](#footnote-136) BREIN moet zich tijdens haar onderzoek ook houden aan de regels van de AVG en UAVG.

# Einde van een tijdperk?

Het Lycos/Pessers-arrest is in Paragraaf 2.8 besproken, maar wat was er nu aan de hand? [[137]](#footnote-137) Dit arrest dateert uit 2005 en is een belangrijk arrest om naw-gegevens op te vragen van tussenpersonen. Sindsdien zijn er verschillende uitspraken geweest, waarvan werd gedacht dat deze het einde van het Lycos/Pessers-tijdperk betekenden.[[138]](#footnote-138) [[139]](#footnote-139) In dit hoofdstuk wordt de tweede deelvraag beantwoord, die luidt: ‘In hoeverre staat het Lycos/Pessers-arrest nog overeind na diverse toetsingen, door zowel politiek als in de hogere rechtspraak, betreffende het verschaffen van naw-gegevens door usenet-, access- en hostingproviders, blijkens wet- en regelgeving en literatuuronderzoek?’[[140]](#footnote-140)

## 3.1 Lycos/Pessers-arrest

Als eerste wordt dieper ingegaan op de zaak van postzegelhandelaar en advocaat Pessers. Hij verkocht postzegels op eBay en werd van fraude beschuldigd op een gratis website van internetprovider Lycos. Pessers spande naar aanleiding hiervan een kort geding aan om achter de naam en het adres van deze persoon te komen. Lycos stelde dat de e-Commercerichtlijn zich in ieder geval tegen een zodanige veroordeling zou verzetten wanneer de gewraakte informatie niet onmiskenbaar onrechtmatig is jegens degene die de vordering instelt. Hieraan ligt art. 15 lid 2 e-Commercerichtlijn ten grondslag, want er is een mogelijkheid dat een isp naw-gegevens moet afgeven aan bevoegde autoriteiten. Dit artikel laat echter niet toe dat de isp gehouden kan worden de gegevens aan civiele partijen te verstrekken.

### 3.1.1 Rechtsregel

De Hoge Raad heeft in dit arrest bepaald dat onder bepaalde omstandigheden de rechtsplicht tot afgifte van de naw-gegevens aan een derde kan bestaan. De Hoge Raad stelde hierop dat de e-Commercerichtlijn geen uitputtende regeling inzake de verstrekking van naw-gegevens bevat. Daarnaast zou de e-Commercerichtlijn niet bedoeld zijn om benadeelden van anonieme onrechtmatige uitingen de gang naar de rechter te ontzeggen. De Hoge Raad bepaalde verder dat de beperking van de aansprakelijkheid van dienstverleners die volgt uit de richtlijn geen afbreuk doet aan de mogelijkheid dat de nationale rechter die maatregelen treft die van deze tussenpersoon redelijkerwijs kunnen worden verlangd in verband met op hem rustende zorgvuldigheidsverplichtingen. Hierbij heeft de Hoge Raad de criteria bevestigd die het Gerechtshof Amsterdam had vastgesteld voor de afgifte van naw-gegevens van isp’s. De vier criteria zijn behandeld in Paragraaf 2.7.

Tussenpersonen kunnen op grond van deze uitspraak niet langer een absoluut weigeringsbeleid voeren. Wanneer een tussenpersoon blijft weigeren, kan hij door de benadeelde aansprakelijk gesteld worden. Dit komt voort uit de op hem rustende zorgvuldigheidsverplichting en heeft als doel om onwettige activiteiten op te sporen en te voorkomen.[[141]](#footnote-141) [[142]](#footnote-142)

### 3.1.2 Gevolgen

Na dit arrest volgden verschillende uitspraken waarin tussenpersonen naw-gegevens moesten afstaan aan de benadeelden. BREIN heeft hierbij ook als benadeelde opgetreden. Deze uitspraken worden in de volgende paragrafen besproken.

## 3.2 Promusicae-arrest

In 2008 volgde het Promusicae-arrest, dat tot veel opschudding leidde.[[143]](#footnote-143) [[144]](#footnote-144) Deze zaak gaat over een vordering van de Spaanse vereniging van muziekproducenten Promusicae. Promusicae vorderde om Telefónica te veroordelen de naw-gegevens van inbreukmakende abonnees te verstrekken. Deze personen gebruikten het zogenaamde peer-to-peerprogramma KaZaA, waarmee volgens Promusicae databestanden konden worden uitgewisseld. Via een map die gedeeld werd vanaf een persoonlijke computer, bood KaZaA aan anderen toegang tot muzieknummers waarvan de exploitatierechten toebehoren aan de leden van Promusicae. Promusicae had de naw-gegevens nodig om civiele procedures tegen de betrokken personen te kunnen instellen.

Telefónica voerde tijdens de zaak aan dat volgens de Spaanse wet de door Promusicae gevraagde gegevens slechts mogen worden verstrekt in het kader van een strafrechtelijk onderzoek of wanneer dit nodig is ter waarborging van de openbare veiligheid en landsverdediging.[[145]](#footnote-145) [[146]](#footnote-146) De Madrileense rechter erkende dit punt, maar verwees de zaak toch door naar het Hof van Justitie om te weten of het gemeenschapsrecht wellicht tot een andere conclusie zou leiden. Hierbij werden de **e-Commercerichtlijn, de Auteursrechtrichtlijn en de Handhavingsrichtlijn specifiek genoemd.**[[147]](#footnote-147)

### 3.2.1 Rechtsregel

Het Hof van Justitie besliste dat er volgens de Algemene privacyrichtlijn in bepaalde gevallen de mogelijkheid is om naw-gegevens te verwerken buiten het doel waarvoor ze zijn verkregen. Dit betekent dat verplichten tot verstrekking van naw-gegevens mág, al hoeft dit niet in civiele zaken. **Geen van de richtlijnen brengt de** verplichting **met zich mee dat lidstaten moeten zorgen dat providers in civiele zaken** naw-gegevens verstrekken.[[148]](#footnote-148) [[149]](#footnote-149) In civiele zaken kan daarom geen algemene verplichting om altijd naw-gegevens te verstrekken, worden opgelegd. Het is echter niet zo dat deze nooit kunnen worden verstrekt. Er moet altijd rekening worden gehouden met mensenrechten en andere beginselen in het gemeenschapsrecht, zoals het evenredigheidsbeginsel. Het gemeenschapsrecht beschermt zowel de privacybelangen van klanten van providers als de rechten van auteursrechthebbenden. Wanneer er een conflict is tussen de twee, moet altijd een afweging worden gemaakt.

## 3.3 Reactie van Ministerie van Justitie en Veiligheid

Het Promusicae-arrest brengt voor Nederland geen veranderingen in de rechtspraak teweeg, volgens het Ministerie van Justitie en Veiligheid.[[150]](#footnote-150) [[151]](#footnote-151) Op verzoek van de vaste Kamercommissie voor Justitie heeft het ministerie een reactie op het Promusicae-arrest geschreven, inhoudende de mogelijke beleidsimplicaties daarvan.[[152]](#footnote-152) Het ministerie geeft aan dat in alle Nederlandse wetgeving op het gebied van intellectueel eigendom een bepaling is opgenomen ter uitvoering van art. 8 lid 1 Handhavingsrichtlijn. Bij een dergelijke bepaling kan een rechter op verzoek van een houder van intellectueel-eigendomsrecht, de betrokken partij bevelen informatie te verstrekken over de herkomst en de distributiekanalen van goederen en diensten die inbreuk maken op intellectueel-eigendomsrecht. Een voorbeeld hiervan is art. 28 lid 9 Aw; in Paragraaf 2.3 zijn andere voorbeelden gegeven.[[153]](#footnote-153)

Richtinggevend voor de Nederlandse situatie is daarbij het arrest Lycos/Pessers-arrest.[[154]](#footnote-154) Daaruit blijkt dat altijd een belangenafweging moet plaatsvinden waarin de grondrechten (waaronder het recht op privacy) worden meegenomen. Volgens het ministerie is er daarom geen reden voor enige beleidswijziging.[[155]](#footnote-155)

## 3.4 Bonnier Audio-arrest

In 2012 volgde echter het Bonnier Audio-arrest.[[156]](#footnote-156) Deze zaak gaat over een kwestie in Zweden. Bonnier Audio, een exploitant van luisterboeken, constateerde dat deze luisterboeken werden uitgewisseld via een ftp-server, een filesharing-programma. Daarop vroeg Bonnier Audio bij de provider ePhone de naw-gegevens op van de persoon achter het IP-adres dat (vermoedelijk) bij deze bestandsuitwisseling was betrokken. ePhone voerde als verweer tegen deze vordering onder meer aan dat het verzochte bevel in strijd is met de Dataretentierichtlijn. Voor de Zweedse rechter was het in hoger beroep onduidelijk of de Dataretentierichtlijn in de weg staat van de toepassing van een op art. 8 Handhavingsrichtlijn gebaseerde nationale bepaling die een isp een dergelijke informatieverplichting oplegt.[[157]](#footnote-157)

### 3.4.1 Rechtsregel

Het Hof van Justitie bepaalde dat de Dataretentierichtlijn alleen regels geeft voor overheidsinstanties. De richtlijn is niet van toepassing op een civiele procedure en daarmee ook niet op de zaak tussen Bonnier Audio en ePhone. Het Hof van Justitie bevestigde vervolgens zijn eerdere Promusicae-uitspraak. In het Bonnier Audio-arrest vond het Hof van Justitie wel dat door middel van art. 8 Handhavingsrichtlijn in combinatie met de e-Privacyrichtlijn het denkbaar is dat rechters een verplichting kunnen opleggen om naw-gegevens vrij te geven. Specifiek moet ervoor worden gewaakt dat het privacybelang van de (beweerdelijk) inbreukmaker moet worden afgewogen tegen het belang van de rechthebbende op de luisterboeken.[[158]](#footnote-158) [[159]](#footnote-159)

## 3.5 Nederlandse rechter

In Nederland kwam er een politieke reactie na het Promusicae-arrest, maar die bleef uit na het Bonnier Audio-arrest.[[160]](#footnote-160) Het duurde tot 2016 voordat een Limburgse voorzieningenrechter zich erover uitliet. Deze rechter bepaalde dat uit beide arresten twee zaken kunnen worden afgeleid. Enerzijds kan geen algemene, op Europese richtlijnen te baseren verplichting worden opgelegd in een gerechtelijke procedure, dat naw-gegevens altijd moeten worden verstrekt. Anderzijds brengen in dit verband relevante Europese richtlijnen niet met zich mee dat die verplichting nooit mag worden opgelegd dan wel dat daarvoor een specifieke nationale regeling is vereist. Daarnaast blijkt uit het Promusicae-arrest en het Bonnier Audio-arrest dat de afgifte van naw-gegevens afhangt van de omstandigheden van het geval en een juiste weging van alle betrokken belangen. Dit is in lijn met het toetsingskader dat in het Lycos/Pessers-arrest is geformuleerd.[[161]](#footnote-161)

## 3.6 Conclusie

Het Lycos/Pessers-arrest is bijna vijftien jaar oud.[[162]](#footnote-162) In de tussentijd is op verschillende momenten gedacht dat het einde van het Lycos/Pessers-tijdperk in zicht was. Echter, na de toetsen van het Hof van Justitie, het Ministerie van Justitie en Veiligheid, en de Nederlandse rechter geldt het Lycos/Pessers-arrest nog steeds.[[163]](#footnote-163) Stichting BREIN kan zich daarom op dit arrest beroepen in haar rechtszaken.[[164]](#footnote-164) In het hoofdstuk Resultaten zal daarom ook gebruik worden gemaakt van het Lycos/Pessers-arrest.

# Resultaten

Uit het Lycos/Pessers-arrest volgen vier criteria voor de afgifte van naw-gegevens door usenet-, access- en hostingproviders.[[165]](#footnote-165) [[166]](#footnote-166) Zoals beschreven in Paragraaf 2.9 is het vierde criterium – het afwegen van de diverse belangen – het lastigst te beoordelen. Deze afweging is afhankelijk van alle omstandigheden die van invloed zijn op het geschil. In dit hoofdstuk wordt duidelijk gemaakt hoe de rechter over de verschillende belangen oordeelt en welk gewicht hij hieraan geeft. Om de zwaarte van de belangen vast te stellen, zijn vijftien relevante uitspraken onderzocht en geanalyseerd. Deze betreffen uitspraken waarvoor usenet-, access- of hostingproviders voor de rechter zijn gedaagd door de benadeelde partij. In dertien zaken is de benadeelde partij de rechthebbende van het werk waarop de inbreuk op auteursrechten is gepleegd. In twee gevallen is de benadeelde partij een tussenpersoon die is aangeschreven door de rechthebbende van het werk. De betreffende tussenpersoon heeft de naw-gegevens niet zelf, maar moet die van de provider van de inbreukmaker verkrijgen, desnoods via een gerechtelijke procedure.

De resultaten zijn verdeeld in verschillende onderwerpen. De onderwerpen voor de verschillende belangen zijn gebaseerd op de belangen volgend uit het Scarlet Extended/SABAM-arrest.[[167]](#footnote-167) [[168]](#footnote-168) Deze onderwerpen betreffen:

* recht op bescherming van eigendom;
* recht op privacy;
* vrijheid van meningsuiting;
* vrijheid van ondernemerschap.

De belangen uit het Scarlet Extended/SABAM-arrest zijn uitgelegd in Paragraaf 2.9.[[169]](#footnote-169) Voor het huidige onderzoek zijn het recht op bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven samengevoegd in het onderwerp ‘recht op privacy’, omdat de Nederlandse rechter of de procespartij deze rechten vaak niet apart benoemt. In Paragraaf 2.9 is ook besproken dat het recht op bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven samen worden gezien als het recht op privacy.[[170]](#footnote-170)

In het onderzoek is niet alleen gekeken naar hoe de verschillende belangen zijn beargumenteerd, maar tevens naar het belang dat volgens de rechter prevaleert. Dit is uitgewerkt onder het onderwerp ‘prevalerend belang’. Ten slotte is het onderwerp ‘bijzonderheden’ toegevoegd. Dit betreft eventuele belangrijke overwegingen van de rechter of argumenten van beide partijen die alleen in een enkele uitspraak zijn benoemd. De uitwerking van deze analyse is te vinden in de Bijlage van dit onderzoek.

## 4.1 Recht op bescherming van eigendom

Het eerste belang dat onderzocht is, betreft het recht op bescherming van eigendom. Dit recht is beschreven in art. 17 lid 2 Handvest. Alle belanghebbenden benoemden dit recht specifiek of dit vloeide voort uit welke juridische stappen de rechthebbenden willen ondernemen tegen de mogelijke inbreukmaker. In alle uitspraken wilde de belanghebbende de inbreukmaker een halt toeroepen. De inbreukmakers plaatsten de content zonder toestemming van de rechthebbenden op grote schaal online, en de verspreiding van deze content zonder toestemming leidde tot ongeautoriseerde openbaarmaking. Hierdoor was sprake van onrechtmatig handelen van de inbreukmaker. Zonder de naw-gegevens konden de rechthebbenden geen juridische acties ondernemen tegen de inbreukmaker met als gevolg dat de inbreuk op de auteursrechten niet stopte.

In één zaak vroeg BREIN de naw-gegevens op van de houders van de BitTorrent-website Sumotorrent. Op deze website werden veel inbreukmakende bestanden aangeboden, zoals films, muziek en games. De rechthebbenden van deze werken hadden geen toestemming verleend voor het delen van deze bestanden, waardoor inbreuk werd gepleegd op de auteursrechten van de aangeslotenen van BREIN. Ook de houders van de website hadden onrechtmatig gehandeld jegens de aangeslotenen van BREIN. Ze hadden welbewust, structureel en stelselmatig gelegenheid geboden tot het uitvoeren van dergelijke inbreukmakende handelingen.[[171]](#footnote-171)

In elf van de dertien zaken spraken de belanghebbenden zich specifiek uit over waarvoor zij de ontvangen naw-gegevens wilden gebruiken. De belanghebbende op wiens content de auteursrechtinbreuk was gepleegd, wilde na ontvangst van deze gegevens tot een overeenkomst komen met de inbreukmaker. Volgens deze overeenkomst betaalt de inbreukmaker een schikkingsbedrag aan de belanghebbende en komen zij overeen dat de inbreukmaker zijn onrechtmatig handelen staakt en gestaakt zal houden.[[172]](#footnote-172) In de overige twee zaken werd niet specifiek benoemd welke juridische acties de rechthebbende zou nemen.

In deze twee zaken was een tussenpersoon de benadeelde partij.[[173]](#footnote-173) In deze gevallen werd de tussenpersoon aangeschreven door de rechthebbende van het materiaal waarop inbreuk werd gepleegd. In een van deze zaken woog de rechter zowel het belang van de tussenpersoon als het belang van de rechthebbende mee. Het belang van de rechthebbende was dat hij zijn auteursrecht op de content die openbaar was gemaakt, wilde beschermen. In deze zaak was XS News gesommeerd door BREIN tot afgifte van de naw-gegevens. Om aan deze sommatie te kunnen voldoen en niet in een gerechtelijke procedure te geraken, daagde XS News Abavia om de naw-gegevens af te geven.[[174]](#footnote-174)

BREIN komt op voor de auteursrechten van haar aangeslotenen en diens leden en voert altijd het recht op bescherming van eigendom aan. Dit blijkt ook uit haar doelstelling, namelijk het bestrijden van auteursrechtinbreuken.[[175]](#footnote-175)

## 4.2 Recht op privacy

Het tweede belang dat onderzocht is, is het recht op privacy. Het recht op bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven vormen samen het recht op privacy.[[176]](#footnote-176) De reden om deze rechten samen te voegen, is omdat in slechts vier zaken deze rechten afzonderlijk aangevoerd werden door de providers. In een van deze zaken beriep de provider zich op beide rechten, op zowel het recht op bescherming van persoonsgegevens als het recht op eerbiediging van het privéleven.[[177]](#footnote-177) In één zaak werd het recht op privacy niet genoemd.[[178]](#footnote-178) De providers hechten dus veel waarde aan de privacy van hun klanten.

In drie zaken gebruikte de provider het argument dat de gegevens van een onschuldige derde zouden kunnen worden opgevraagd.[[179]](#footnote-179) Het IP-adres kon bijvoorbeeld inmiddels door een andere onschuldige partij worden gebruikt. De klant van de provider waar de naw-gegevens werden opgevraagd, zou volgens de provider niet de auteursrechtelijke werken online plaatsen. Wanneer de provider de naw-gegevens zou afstaan, kon de rechthebbende een onschuldige partij aanschrijven, terwijl de echte inbreukmaker kon doorgaan met het plaatsen van auteursrechtelijke werken. In een van deze zaken werd daarom gesproken van een ‘onomkeerbare situatie’.[[180]](#footnote-180)

In dezelfde zaak (tegen UPC) vroeg BREIN drie e-mailadressen op. UPC voerde aan dat het derde e-mailadres in eerste instantie wel gebruikt was door de inbreukmaker om zich aan te melden, maar dat de betrokkene dit e-mailadres zelf had aangemaakt, niet UPC. Dit zogenoemde ‘secundaire’ e-mailadres kan te allen tijde gewijzigd worden zonder dat UPC daarvan een administratie bijhoudt. UPC had kunnen constateren dat dit secundaire e-mailadres online was ten tijde van de rechtszaak, maar kon niet weten sinds wanneer dat het geval was en daarom ook niet of dit een onafgebroken periode was geweest. De inbreukmaker had bijvoorbeeld de dag na zijn aanmelding zijn account kunnen opheffen, waarna het e-mailadres voor een ander beschikbaar werd. De inbreukmaker gebruikte de naam Muzan, wat een vrij veelvoorkomende Arabische naam is.[[181]](#footnote-181) Hierdoor bestond een gerede kans dat een derde, ‘onschuldige’ gebruiker het adres had kunnen overnemen.[[182]](#footnote-182)

BREIN moet dus de onzekerheid bij providers wegnemen. Ze moet bewijzen dat een account gekoppeld is aan de inbreukmaker en dat hier geen nieuwe partij aan verbonden is. Dit moet tijdens de bewijsverzameling goed worden vastgesteld. Om verrassingen tijdens het proces over het opvragen van naw-gegevens te voorkomen, moet dit een doorlopend proces zijn. Hierdoor kan BREIN bewijzen dat de kans dat een onschuldige derde de accounthouder is nihil is.

In een zaak voerde de usenetprovider aan dat hij zo min mogelijk gegevens van zijn klanten wilde verzamelen. Wanneer klanten een abonnement bij deze provider afsloten, konden zij content van usenet downloaden en bestanden naar usenet uploaden. Voor de bedrijfsvoering had de usenetprovider alleen een e-mailadres en een bankrekening van de klant nodig, in het kader van dataminimalisatie. In deze zaak werden alleen de naw-gegevens en het e-mailadres opgevraagd. Via een screenshot van het formulier dat een klant moet invullen als hij een abonnement aangaat bij de usenetprovider, kon ook bewezen worden dat deze gegevens gevraagd waren door de betreffende provider.[[183]](#footnote-183)

Wanneer dit argument wordt aangevoerd, moet BREIN onderzoeken om welke gegevens deze provider de klant vraagt bij het afsluiten van een abonnement. Dit staat op de website van de betreffende provider zelf, bijvoorbeeld als het inschrijfformulier en BREIN moet dit als bewijs vastleggen. Het bewijs kan een screenshot zijn van een formulier dat een klant moet invullen om een abonnement af te sluiten. Uit dit formulier moet blijken dat de gevraagde gegevens ook worden verzameld door een provider die dataminimalisatie betracht. In de eerdergenoemde zaak oordeelde de rechter dat er geen overbodige informatie was gevraagd; hiermee doelde de rechter op kopieën van identiteitsbewijzen, bsn-nummers et cetera.[[184]](#footnote-184)

BREIN moet er dus zelf voor zorgen dat zij in haar verzoek tot afgifte van naw-gegevens bij een provider geen overbodige informatie vraagt. Een provider beschikt altijd over de betaalgegevens en een e-mailadres of postadres van een klant om contact met hem te kunnen houden. BREIN moet voor de opgevraagde gegevens zelf bepalen welke zij nodig heeft om de inbreukmaker die auteursrechtelijke werken online verspreidt, te kunnen aanschrijven.

In vier zaken meende de provider dat hij zelf geen goede belangenafweging kon maken voor het verstrekken van de naw-gegevens doordat het verzoek van de rechthebbende tot afgifte van de naw-gegevens van de inbreukmaker te summier was geformuleerd of provider anders te lichtvaardig met privacygevoelige gegevens zou omgegaan.[[185]](#footnote-185) [[186]](#footnote-186) Wanneer een provider bij BREIN aangeeft dat het verzoek tot afgifte van de naw-gegevens van de inbreukmaker te summier geformuleerd is, kan BREIN haar bewijsmateriaal uitbreiden en een duidelijk overzicht maken van wat de inbreukmaker heeft gedaan en welke gegevens BREIN wil hebben. BREIN moet hierbij ook duidelijk beargumenteren waarom zij de gevraagde gegevens nodig heeft en waarom juist die gevraagde gegevens en niet minder gegevens nodig zijn.

In drie zaken haalden de providers aan dat de houders van een inbreukmakend platform er belang bij hebben om anoniem te blijven. De houder van het platform wil op internet contacten leggen en gegevens uitwisselen zonder het risico te lopen dat zijn identiteit ongewenst onthuld wordt door de provider aan wie hij zijn naw-gegevens heeft verstrekt. In alle drie de zaken weerlegde de rechter dat de anonimiteit niet misbruikt mag worden om jegens derden onrechtmatig te handelen zonder dat de inbreukmaker daarvoor ter verantwoording kan worden geroepen.[[187]](#footnote-187) In een van deze zaken beargumenteerde de rechter ook dat het onrechtmatig handelen van de inbreukmaker anders in de praktijk onbeperkt voortgezet kan worden. Daarom dient het belang om iemands identiteit anoniem te houden daarvoor te wijken.[[188]](#footnote-188)

Wanneer BREIN een verzoek doet bij een provider tot afgifte van de naw-gegevens van de houder van een inbreukmakend platform, moet ze de onrechtmatigheid van de website, het onrechtmatig handelen van de houder en de mate van de inbreuk bewijzen. Uit het verzoek van BREIN tot afgifte van de naw-gegevens moet duidelijk blijken dat het onrechtmatig handelen van het platform en de houder hiervan onbeperkt zullen doorgaan indien deze gegevens niet verstrekt worden aan BREIN.

In een zaak beriep de rechthebbende die de auteursrechten bezat van het werk waarop inbreuk was gepleegd zich op art. 28 lid 9 Aw. Dit artikel, dat is besproken in Paragraaf 2.6, vormt een bij wet geregelde beperking van het recht op bescherming van persoonsgegevens en beperking van de eerbiediging van de persoonlijke levenssfeer. Bij de belangenafweging laat de rechter deze twee rechten daarom buiten beschouwing.[[189]](#footnote-189) BREIN kan hiermee rekening houden wanneer zij in het vervolg naw-gegevens vordert op grond van art. 28 lid 9 Aw. Op basis van dit artikel moet dat wel via een rechterlijk bevel.

## 4.3 Vrijheid van meningsuiting

Het derde belang dat onderzocht is, is de vrijheid van meningsuiting en informatievrijheid. Deze vrijheid is beschreven in art. 11 Handvest. Zeven keer werd deze vrijheid aangevoerd door een provider. In twee zaken wilde de provider een platform aanbieden waarop in vrijheid de informatie van derden verspreid kon worden en zodat hij niet veroordeeld kon worden om privacygevoelige gegevens van zijn gebruiker te moeten afgeven. Het usenet bestaat uit een groot aantal servers over de gehele wereld, die onderling met elkaar verbonden zijn en informatie uitwisselen. Commerciële usenetproviders bieden tegen betaling toegang tot usenet en zorgen dat hun klanten content op usenet kunnen uitwisselen. In een van deze twee zaken wilde Eweka zijn klanten zeven en een half jaar retentie geven, wat inhoudt dat vrijwel alle content die naar usenet was geüpload tot in ieder geval zeven en een half jaar terug te vinden was op de servers van Eweka. In dezelfde zaak bood Usenetter zijn diensten ook aan onder de naam Extreme Usenet en bood de provider zijn klanten retentie tot drie jaar.[[190]](#footnote-190)

In vier zaken benoemde de rechter de vrijheid van meningsuiting. In die uitspraken is niet te lezen dat de provider dit belang zelf had aangevoerd. In deze uitspraken gaf de rechter aan dat de vrijheid van meningsuiting niet zover gaat dat de klant van de provider het recht heeft om anoniem inbreuk te maken op de auteursrechten van de rechthebbende.[[191]](#footnote-191) Voor BREIN is dit een belangrijk punt. Ze moet duidelijk kunnen aantonen dat de klant veel inbreuk maakt op de auteursrechten van haar rechthebbende. BREIN moet daarvoor veel bewijs vastleggen van het inbreukmakende handelen van de inbreukmaker. Op het moment dat BREIN dit duidelijk kan aantonen, vervalt het argument van de provider dat de naw-gegevens niet kunnen worden afgegeven omdat anders inbreuk wordt gemaakt op de vrijheid van meningsuiting van de klant.

## 4.4 Vrijheid van ondernemerschap

Het vierde belang is de vrijheid van ondernemerschap, dat is beschreven in art. 16 Handvest. In vier zaken werd dit recht niet specifiek benoemd. In de gevallen dat het wel was benoemd, werd gesteld dat de provider niet in staat was om een belangrijke afweging te maken. Voor de provider staat veel op het spel. De provider mag niet zomaar gegevens van zijn klanten afstaan. Wanneer klanten zien dat een provider gegevens afstaat aan een organisatie als BREIN, zullen sommige misschien overstappen. De verschillende redenen van providers om niet zomaar gegevens af te staan zijn: het verzoek is te summier, het verzoek is te belastend qua tijd en geld, of de provider heeft te weinig informatie om een afweging te kunnen maken.

Om het argument van de provider te weerleggen dat het verzoek te summier is of dat te weinig informatie gegeven is, kan BREIN additioneel bewijs aanleveren om de mate van de inbreuk door de inbreukmaker aan te tonen. Daarbij moet BREIN duidelijk zijn over welke gegevens ze nodig heeft. De provider kan het verzoek niet meer summier vinden wanneer BREIN dit additionele bewijs met extra verduidelijking aan hem geeft. Om het argument dat het verzoek veel tijd en geld kost, te weerleggen, kan BREIN de noodzaak duidelijk maken. Verder kan BREIN aangeven dat zij anders naar de rechter toe zal stappen, waardoor het verzoek alleen maar meer tijd en geld gaat kosten.

BREIN vraagt de provider in elk verzoek tot afgifte van naw-gegevens, dit verzoek ook door te sturen naar de desbetreffende klant. Tevens vermeldt BREIN dat wanneer de klant geen contact opneemt met BREIN, dat de provider zal worden verzocht tot afgifte van de naw-gegevens. Op deze manier probeert BREIN kosten en tijd te besparen. Wanneer de klant uit zichzelf contact opneemt met BREIN, hoeft de provider niet de afweging te maken over de afgifte van de naw-gegevens.

In vier zaken haalde de provider aan dat hij alle beschikbare gegevens van de inbreukmaker al had afgestaan aan de rechthebbende op wiens werk auteursrechtinbreuk was gepleegd en/of dat niet over verdere gegevens beschikte. Een argument van de provider waarom hij niet over gegevens beschikte, was dat de klant altijd op tijd had betaald.[[192]](#footnote-192) BREIN kan hierbij als tegenargument gebruiken dat indien de klant op tijd betaalt, er betaalgegevens aanwezig moeten zijn. Bij het aangaan van een abonnement zijn heeft de klant correcte gegevens afgegeven aan de provider om de overeenkomst te kunnen bevestigen. De provider zal zelf ook correcte gegevens willen hebben in het geval de klant zich niet houdt aan diens verplichtingen.

In twee zaken gaf de provider aan dat hij bij afgifte van naw-gegevens reputatieschade zou oplopen. Een provider kan aansprakelijk worden gesteld wanneer hij zonder zwaarwegende grond persoonsgegevens afgeeft aan derden. Deze zwaarwegende grond was volgens de provider niet aanwezig.[[193]](#footnote-193) In Paragraaf 2.2.1 is behandeld dat een tussenpersoon kan worden gevrijwaard, maar dat een rechterlijk verbod of gebod niet kan worden uitgesloten. De provider heeft daarnaast belang bij het behouden van zijn klant.[[194]](#footnote-194)

In een zaak haalde de provider aan dat de klantrelatie met de mogelijke inbreukmaker inmiddels was verbroken. De provider was daarom gehouden om de naw-gegevens te vernietigen. De provider had de klantgegevens nog wel, maar volgens de provider was dit feitelijk onrechtmatig.[[195]](#footnote-195) BREIN moet na het vaststellen van de inbreuk en het achterhalen bij welke usenetprovider de inbreukmaker gebruikt, zo snel mogelijk een verzoek indienen bij de desbetreffende provider, zodat de benodigde gegevens bewaard worden. Bij voldoende bewijsmateriaal moet de provider de gegevens dan alsnog afstaan.

## 4.5 Prevalerend belang

Het vijfde onderwerp dat onderzocht is, is welk belang de rechter vindt dat prevaleert. De rechter weegt bij zijn oordeel alle voorgaande grondrechten mee om tot een oordeel te komen. Volgens het vierde criterium van het Lycos/Pessers-arrest behoort het belang van de derde te prevaleren om naw-gegevens te verkrijgen.[[196]](#footnote-196)

In elf zaken prevaleerde het belang van de belanghebbende op wiens werk auteursrechtinbreuk was gepleegd. De provider moest daardoor de naw-gegevens afstaan aan de rechthebbende. De rechter baseerde zich hierbij op de volgende uitgangspunten. In drie zaken woog het belang van de rechthebbende zwaarder, omdat de inbreukmaker ter verantwoording moet kunnen worden geroepen voor zijn onrechtmatig handelen. In een van deze zaken had de inbreukmaker niet voldaan aan een notice-and-take-down-verzoek van de rechthebbende.[[197]](#footnote-197) In vijf zaken oordeelde de rechter dat het belang van de rechthebbende prevaleerde, omdat de inbreuk van de inbreukmaker op de auteursrechten van de rechthebbende omvangrijk was. In een van deze vijf zaken oordeelde de rechter dat een zichzelf respecterende usenetprovider niet geassocieerd wil worden met dergelijk grootschalig onrechtmatig handelen.[[198]](#footnote-198) In twee zaken benoemde de rechter specifiek de zorgvuldigheidsverplichting. Wanneer de provider de gegevens niet af zou staan, handelde hij in strijd met zijn zorgvuldigheidsverplichting. Ten slotte oordeelde de rechter in een geval dat het belang van de rechthebbende prevaleerde, omdat de inbreukmaker na het blokkeren van zijn account door de aangeschreven usenetprovider de inbreuk via een andere usenetprovider had voortgezet.[[199]](#footnote-199)

In vier gevallen prevaleerde het belang van de provider. In een van deze zaken had de belanghebbende de gegevens op een onjuiste manier verzameld en verwerkt.[[200]](#footnote-200) Bij een andere uitspraak was er een alternatieve mogelijkheid om de gevraagde naw-gegevens te verkrijgen die minder ingrijpend was.[[201]](#footnote-201) In de zaak van DFW, zoals eerder besproken in Hoofdstuk 1, had de filmdistributeur onvoldoende duidelijk gemaakt op welke wijze hij de IP-adreshouders wilde benaderen. DFW wist nog niet of hij de IP-adreshouder kon aanmerken als downloader. Het was tevens onduidelijk of een voor te stellen schikkingsbedrag wel overeenkwam met de feitelijke schade. Ten slotte was niet duidelijk wat DFW aan de IP-adreshouder zou mededelen omtrent de rechten en plichten van de IP-adreshouders.[[202]](#footnote-202)

Verder is het opvallend dat de zaken waarin de rechthebbende het recht op bescherming van eigendom gebruikt tegen een inbreuk waardoor meerdere rechthebbenden schade lijden vaker worden toegewezen dan wanneer er één rechthebbende is. Blijkbaar weegt de rechter in zijn afweging van de verschillende belangen dus ook mee hoeveel rechthebbenden schade lijden door de inbreuk.

## 4.6 Bijzonderheden

In een aantal zaken vallen ook andere punten op. Deze punten kwamen alleen voor bij specifieke uitspraken en zijn daarom niet als apart onderwerp onderzocht.

In een zaak sprak de belanghebbende over het recht op effectieve rechtsbescherming.[[203]](#footnote-203) Dit recht vloeit voort uit art. 47 Handvest en art. 13 EVRM. Het beginsel houdt in dat particulieren in staat moeten zijn om rechten die zij aan het Europese recht ontlenen voor de rechter in te roepen.[[204]](#footnote-204) Art. 47 Handvest luidt: ‘*Eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, heeft recht op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden.’* Indien BREIN dit argument gebruikt, zal dit waarschijnlijk in hoger beroep zijn, omdat BREIN in eerste aanleg vond dat zij geen effectieve rechtsbescherming kreeg van de rechter. Dit argument zal waarschijnlijk niets toevoegen aan de rechtszaak. In de drie overige uitspraken in hoger beroep werd dit argument niet gebruikt. In de literatuur staat ook dat het belangrijkste grondrecht van de rechthebbende het recht op bescherming van eigendom betreft.[[205]](#footnote-205)

In Paragraaf 2.2.1 is besproken dat uit art. 6:196c lid 4 BW een vrijstelling van aansprakelijkheid voor tussenpersonen vloeit. Aan deze vrijstelling zijn voorwaarden gesteld. In een van de uitspraken voerde de provider aan dat op grond van dit artikel de naw-gegevens niet mogen worden afgestaan. De rechter bepaalde dat deze vrijstelling niet van toepassing was in deze zaak. Een van de voorwaarden van vrijwaring is dat de tussenpersoon de toegang onmogelijk maakt of de informatie verwijdert wanneer de provider op de hoogte wordt gesteld van de onrechtmatigheid. In deze zaak was de provider meerdere malen op de hoogte gebracht door BREIN. Hierdoor voldeed de provider niet aan de voorwaarde van vrijwaring van aansprakelijkheid.[[206]](#footnote-206) Wanneer de provider weigert om de gevraagde gegevens af te staan, moet BREIN de ernst van de zaak duidelijk maken door te volharden en aanvullend bewijs te versturen om de gevraagde informatie te verkrijgen.

In een van de zaken werd een provider gevraagd om niet alleen informatie te verstrekken over een specifieke website, maar ook over de dienstverlening met betrekking tot andere websites. De rechter bepaalde dat de provider de informatie over de specifieke website moest afgeven, maar dat hij de informatie over de dienstverlening met betrekking tot andere websites niet hoefde te delen.[[207]](#footnote-207) Voor BREIN betekent dit dat in haar verzoek niet meer informatie moet vragen dan nodig is.

In een aantal uitspraken voerde de belanghebbende aan dat de provider zelf de beoordeling tot afgifte van naw-gegevens had kunnen toetsen aan de hand van het Lycos/Pessers-arrest. In één zaak vond de provider dat hij de belangenafweging niet zelf kon uitvoeren, maar de rechter oordeelde daar anders over. De belanghebbende had bewijsmateriaal aangedragen waaruit opgemaakt kon worden dat er grootschalig inbreuk werd gepleegd op de rechten van de rechthebbende van de werken.[[208]](#footnote-208) BREIN moet in haar verzoek de mate van de inbreuk op de auteursrechten van haar rechthebbende duidelijk maken aan de providers. Ook moet ze ervoor zorgen dat de provider genoeg informatie heeft, zodat de provider zelf de afweging kan maken. Hierdoor komt het argument dat de provider de afweging niet zelf kan maken, te vervallen.

In een andere uitspraak bepaalde de rechter dat een usenetprovider moet kunnen beschikken over identificerende gegevens van personen die beschermde inhoud hebben geüpload. Dit moet de usenetprovider bereiken door bij het sluiten van een overeenkomst met een bedrijf waar hij serverruimte huurt, te bedingen dat dit bedrijf deze informatie doorgeeft. Anders handelt de usenetprovider in strijd met zijn zorgvuldigheidsverplichting.[[209]](#footnote-209) BREIN weet door deze uitspraak dat de provider altijd over identificerende gegevens van zijn klanten moet beschikken. Zoals in Paragraaf 4.4 is besproken, voerde een provider als argument aan dat hij de gevraagde gegevens niet had. In een dergelijke situatie kan BREIN beargumenteren dat dit tegen de zorgvuldigheidsverplichting van de provider ingaat.

In de twee recentste uitspraken werd de AVG genoemd; de belangrijkste veranderingen na de invoering van de AVG zijn besproken in Paragraaf 2.10. De AVG is relatief nieuw, waardoor ten tijde van dit onderzoek in totaal drie rechtszaken zijn gevoerd waarin naw-gegevens werden gevorderd. In de derde zaak ging het niet om een provider, maar om een ander soort tussenpersoon.[[210]](#footnote-210) In een van deze uitspraken werd benoemd dat de verwerking van persoonsgegevens door de eiser, in dit geval DFW, rechtmatig was. Ook werd geoordeeld dat DFW heeft gehandeld volgens hun protocol en de AVG.[[211]](#footnote-211) In het hoger beroep werd ook de verwerking van persoonsgegevens door Ziggo nader onderzocht.[[212]](#footnote-212) BREIN moet zorgen dat zij voldoet aan de AVG-regelgeving. Deze drie rechtszaken vormen nog geen leidraad hoe de AVG en UAVG wordt getoetst tijdens een zaak over afgifte van naw-gegevens.

## 4.7 Conclusie

Het laatste criterium van het Lycos/Pessers-arrest, de belangenafweging, is het belangrijkste. Volgens dit vierde criterium behoort het belang van de derde te prevaleren om naw-gegevens te verkrijgen.[[213]](#footnote-213) Om een goede belangenafweging te kunnen maken, is het van belang dat de rechthebbende weet welke juridische stappen hij zal nemen wanneer hij de naw-gegevens heeft ontvangen. De rechter moet oordelen dat het recht op bescherming van eigendom zwaarder weegt. Deze beslissing is grotendeels afhankelijk van de ernst van de inbreuk en of er sprake is van een meervoudige of enkelvoudige inbreuk.

De rechter oordeelt dat wanneer er sprake is van inbreuk op auteursrechten, de klant zich niet kan verschuilen achter de vrijheid van meningsuiting; vaak de rechter dit argument buiten hij. Wanneer de provider zich beroept op de vrijheid van ondernemerschap en aangeeft dat men niet zelf de belangenafweging kan maken, wordt ook dit argument meestal buiten beschouwing gelaten. De rechter heeft namelijk geoordeeld dat de provider deze belangenafweging zelf kan én moet maken.

De rechter neemt vaak wel het recht op privacy mee in de beoordeling. Wanneer BREIN zich echter beroept op art. 28 lid 9 Aw, kan het recht op privacy ook buiten beschouwing gelaten worden. Wanneer BREIN zich beroept op dit artikel, moet ze wel een bevel van de rechter verkrijgen. In dit bevel wordt de provider bevolen de naw-gegevens van de inbreukmaker aan BREIN af te geven.

Om ervoor te zorgen dat het belang van BREIN prevaleert, is het essentieel dat BREIN de gegevens rechtmatig verwerkt. Hierbij zijn de AVG en het eigen protocol relevant. Uit de rechtspraak blijkt ook dat een provider zelf kan en moet beoordelen of voldaan is aan de criteria uit het Lycos/Pessers-arrest om te voorkomen dat hij niet voldoet aan de zorgvuldigheidsverplichting die op hem rust.

BREIN moet in haar verzoek het bewijsmateriaal goed vastleggen en zich houden aan de privacywetgeving, zodat de verwerkte gegevens rechtmatig verkregen worden. In haar verzoek moet BREIN ook duidelijk maken welke auteursrechtelijke content de inbreukmaker op internet heeft geplaatst en wat de mate van de inbreuk is. Verder moet BREIN alleen om die gegevens vragen die zij nodig heeft en niet om gegevens waar ze geen recht op heeft, omdat deze als overbodig kunnen worden aangemerkt. In haar verzoek moet BREIN ook mogelijke twijfel bij een provider wegnemen door het aanleveren van bewijs dat de inbreukmaker achter het betreffende IP-adres of e-mailadres zit.

# Conclusie

Deze afstudeeropdracht heeft als doel BREIN te adviseren over de afgifte van naw-gegevens van inbreukmakers door usenet-, access- en hostingproviders. De reden hiervoor is de belangenafweging door de rechter die volgt uit het vierde criterium van het Lycos/Pessers-arrest.[[214]](#footnote-214) Uit jurisprudentie is gebleken dat het belang van de belanghebbende niet altijd prevaleert. De centrale vraag van dit onderzoek luidt: ‘Wat kan aan Stichting BREIN worden geadviseerd met betrekking tot de afgifte van naw-gegevens door usenet-, access- en hostingproviders, blijkens wet- en regelgeving, literatuuronderzoek en jurisprudentieonderzoek?’

BREIN heeft twee opties om naw-gegevens van inbreukmakers op te vragen bij usenet-, access- en hostingproviders. De strafrechtelijke mogelijkheid is niet van belang voor BREIN, omdat auteursrecht geen prioriteit heeft. De eerste optie is dat BREIN direct bij de provider de naw-gegevens opvraagt op basis van art. 6:162 BW in combinatie met het Lycos/Pessers-arrest.[[215]](#footnote-215) De tweede optie is dat ze de naw-gegevens verkrijgt via een rechterlijk bevel op basis van art. 28 lid 9 Aw. Beide opties om de naw-gegevens te verkrijgen van personen die onrechtmatig content van de rechthebbenden van BREIN op internet hebben gezet, hebben voor- en nadelen.

Bij beide opties is het van belang dat BREIN zich houdt aan de regelgeving van de AVG. Relevant hierbij is de rechtmatigheid van de verwerking van persoonsgegevens. Verder moet BREIN ervoor zorgen dat zij aan haar verantwoordingsplicht voldoet, wat betekent dat de verantwoordelijkheid om aan te tonen dat BREIN aan de AVG voldoet bij haar ligt. BREIN moet kunnen aantonen dat ze bij de verwerking van persoonsgegevens de AVG-regelgeving in acht heeft genomen. Daarom is goede documentatie essentieel. Ook moet BREIN rekening houden met het recht van bezwaar doordat ze gegevens verwerkt op grond van art. 6 lid 1 sub f AVG. Echter, is het recht van bezwaar niet geldig wanneer BREIN een rechterlijk bevel heeft. De AVG is bijna twee jaar geleden ingevoerd, maar hoe deze wet samen met de UAVG wordt behandeld in een zaak tot afgifte van naw-gegevens door providers is nog onzeker. Op dit moment zijn er nog maar drie zaken over hoe de AVG en UAVG worden behandeld bij het opvragen van naw-gegevens geweest.[[216]](#footnote-216) [[217]](#footnote-217) [[218]](#footnote-218) In deze zaken heeft de rechter wel bekeken of de door de partijen verkregen gegevens rechtmatig waren verwerkt

Bij de eerste optie kan BREIN de naw-gegevens opvragen van de inbreukmaker bij de provider op basis van art. 6:162 BW, oftewel de onrechtmatige daad. De onrechtmatige daad moet in combinatie met het Lycos/Pessers-arrest worden gebruikt.[[219]](#footnote-219) In dit arrest worden vier criteria genoemd waaraan voldaan moet worden voor de afgifte van naw-gegevens van een inbreukmaker. Het eerste criterium is dat de informatie aannemelijk onrechtmatig en schadelijk is. Met de informatie wordt bedoeld dat de inbreukmaker het werk van de rechthebbende openbaar maakt of verveelvoudigt. Het tweede criterium is dat de benadeelde partij een reëel belang heeft bij afgifte van de naw-gegevens. In dit criterium wordt bedoeld dat de benadeelde partij, oftewel de partij die de naw-gegevens vordert, de rechthebbende is van het werk waarop auteursrechtinbreuk is gepleegd of voor hem mag optreden. Het derde criterium is dat er geen minder ingrijpende mogelijkheden zijn. Dit betekent dat als er gegevens bekend zijn, zoals een mailadres, BREIN eerst contact probeert op te nemen via het mailadres. Het laatste criterium is dat het belang van de benadeelde prevaleert boven dat van de inbreukmaker en de provider. Wanneer aan deze criteria voldaan wordt, moet de provider de naw-gegevens afgeven.

Het laatste criterium van het Lycos/Pessers-arrest, de belangenafweging, is het belangrijkste. De rechter weegt het belang van de rechthebbende, namelijk het recht op bescherming van eigendom, af tegen het recht op bescherming van persoonsgegevens, het recht op eerbiediging van het privéleven, de vrijheid van meningsuiting en de vrijheid van ondernemerschap. Hierbij is het van belang dat de rechthebbende duidelijk maakt waarvoor hij de naw-gegevens zal gebruiken. Of de rechter oordeelt dat het recht op bescherming van eigendom prevaleert, is grotendeels afhankelijk van de ernst van de inbreuk en of er sprake is van een meervoudige of enkelvoudige inbreuk.

Op grond van de onrechtmatige daad in combinatie met het Lycos/Pessers-arrest kan BREIN direct naar de provider toe. De rechter heeft in verschillende zaken geoordeeld dat een provider zich niet kan verschuilen achter het argument dat hij niet zelf de belangenafweging kan maken. Dit vloeit voort uit de op hem rustende zorgvuldigheidsverplichting en heeft tot doel onwettige activiteiten op te sporen en te voorkomen. Wanneer de provider echter weigert om de naw-gegevens af te geven, kan dit een langdurig proces worden. Dan zal BREIN alsnog naar de rechter moeten om de naw-gegevens van de inbreukmaker te verkrijgen van de provider. Tevens kan bij deze optie de mogelijke inbreukmaker zich beroepen op het recht van bezwaar bij de provider. Dit is het geval wanneer de provider wel de naw-gegevens zou willen afgeven en de inbreukmaker hierover wil inlichten. Hierdoor kan het ook een langdurig proces worden en is het mogelijk dat de gegevens uiteindelijk gewist worden.

Bij de tweede optie om naw-gegevens op te vragen op basis van art. 28 lid 9 Aw, moet BREIN altijd naar de rechter om een rechterlijk bevel te krijgen. BREIN zal dan direct naar de rechter moeten gaan en kan niet eerst de provider vragen om vrijwillig de naw-gegevens van de inbreukmaker af te staan. Bij deze optie wordt er nog steeds getoetst aan de criteria van het Lycos/Pessers-arrest, maar het recht op privacy wordt achterwege gelaten door de geregelde beperking uit art. 28 lid 9 Aw. Verder vervalt ook het recht van bezwaar uit de AVG.

Uiteindelijk zijn er dus twee opties voor BREIN om naw-gegevens op te vragen.

# Aanbevelingen

In dit hoofdstuk worden aanbevelingen aan opdrachtgever Stichting BREIN gegeven. Deze aanbevelingen vloeien voort uit de conclusie.

De eerste aanbeveling is om te onderzoeken of het goedkoper, eenvoudiger en sneller is om direct bij de rechter een verzoek tot afgifte van de naw-gegevens van de inbreukmaker in te dienen. Mogelijk is dit goedkoper wanneer een provider de naw-gegevens niet vrijwillig wil afgeven. De tijd die de werknemers van BREIN hebben gestoken in het contact met de provider en daarna in de rechtszaak wordt daardoor verminderd. Ook kan een directe gang naar de rechter eenvoudiger zijn, omdat art. 28 lid 9 Aw ervoor zorgt dat het recht op privacy buiten beschouwing blijft. Wanneer BREIN de inbreuk op de auteursrechten van haar rechthebbenden wil stoppen, treedt BREIN op voor een meervoudige inbreuk. BREIN treedt op voor meerdere rechthebbenden en wanneer meerdere onrechtmatige werken worden aangeboden. Hierdoor is de kans groter dat de rechter in haar voordeel beslist. Het proces tot het verkrijgen van de naw-gegevens van een provider zal op deze manier waarschijnlijk sneller gaan dan wanneer BREIN eerst contact zoekt met de provider. De provider kan weigeren om de naw-gegevens af te staan, omdat hij vindt dat zijn belang en dat van zijn klant zwaarder weegt dan het belang voor het verkrijgen van de naw-gegevens van BREIN. Aangezien de inbreukmaker niet direct kan worden aangesproken, duurt de inbreuk voort.

De tweede aanbeveling heeft betrekking op de situatie waarin BREIN er toch voor kiest om direct naar de provider te gaan met haar verzoek tot afgifte van de naw-gegevens van de (mogelijke) inbreukmaker. Als deze (mogelijke) inbreukmaker bezwaar heeft aangetekend bij de provider, kan BREIN het beste naar de rechter gaan. Anders kan het in de procedure van het recht van bezwaar van de AVG lang duren voordat wordt overgegaan tot eventuele afgifte van de naw-gegevens, waardoor de inbreuk eventueel kan doorgaan. Tevens kan, op het moment dat de provider oordeelt dat de (mogelijke) inbreukmaker gelijk heeft dat zijn naw-gegevens niet mogen worden afgegeven, deze (mogelijke) inbreukmaker zich beroepen op het feit dat zijn gegevens moeten worden gewist.

De derde aanbeveling is om de AVG en UAVG goed na te leven. Verder dient BREIN de relevante jurisprudentie hierover in de gaten te houden. Als BREIN onrechtmatig persoonsgegevens verwerkt, zal zij niet alleen de naw-gegevens niet verkrijgen, maar ook loopt ze de kans op ene boete en reputatieschade. Doordat de AVG relatief nieuw is en besproken is in maar drie uitspraken bij afgifte van naw-gegevens is hier is geen duidelijke jurisprudentie voor. Van belang hierbij is hoe de rechter de AVG toetst bij het opvragen van naw-gegevens; dit is op dit moment onduidelijk. BREIN moet zich houden aan de verplichtingen die voortvloeien uit de AVG en UAVG. Hierbij is het van belang dat BREIN haar registers bijhoudt en indien nodig vernieuwt. Op deze manier is de verwerking van naw-gegevens tijdens een onderzoek altijd rechtmatig.

De vierde en laatste aanbeveling is dat BREIN het stroomschema op de volgende pagina volgt in haar onderzoeken.



# Bronnenlijst

**Literatuur**

Radar AVROTROS, augustus 2016.

AVROTROS, ‘*Tevreden lezers van (vaak illegale) e-books*’, 9 augustus 2016.

Alberdingk Thijm en De Vries, BIE 2015.

C. Alberdingk Thijm en C. de Vries, ‘De toenemende invloed van het Handvest op het recht van intellectuele eigendom’ BIE september 2019, pag. 174-183.

Bauch, e.a., 1999.

L. Bauch, M. Green & M. Wyburn, *The Boundaries of Copyright*, Sydney 1999.

Berkvens & Jakimowicz, 2018.

J. Berkvens & C. Jakimowicz, ‘*Tekstuitgave privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen*’, Den Haag: Boom Juridische uitgevers 2016.

Brinkhof, *NJB* 1994.

J.J. Brinkhof, ‘*Codificatie van het recht van de intellectuele eigendom*?’, NJB 1994, pag. 771-779.

Chavannes, AMI 2015/2.

R.D Chavannes, ‘‘Juist evenwicht’ in de praktijk’, AMI 2015/2, pag. 38-47.

Dijkstra, 2008.

C.N.J. de Vey Mestdagh & J.J. Dijkstra, *ICT-recht voor de praktijk*, Groningen/Houten: Noordhoff Uitgevers 2008.

Dommering, 2011.

E.J. Dommering, ‘De zaak Scarlet/Sabam – Naar een horizontale integratie van het auteursrecht’, AMI 2011-2, pag. 49-53.

Protocol, 6 juli 2017.

Dutch FilmWorks B.V., *‘Protocol -Online handhaving intellectuele eigendomsrechten’,* 6 juli 2017.

Engelfriet, e.a. 2019.

A. Engelfriet, L. Meij & P. Krager, ‘*De Algemene verordening gegevensbescherming (AVG). Artikelsgewijs commentaar*’, IUS Mentis, 2019.

Geerts, 2019.

P.G.F.A. Geerts, *Bescherming van de intellectuele eigendom*, Deventer: Wolters Kluwer 2019.

Gellaerts & Jobse, 2019.

S.L. Gellaerts & C.M. Jobse, *Inleiding ICT en recht*, Deventer: Wolters Kluwer 2019.

Gielen, e.a., 2018.

Ch. Gielen, A.C.M. Alkema, P.G.F.A. Geerts, *Kort begrip van het intellectuele eigendomsrecht*, Deventer: Wolters Kluwer, 2018.

Asser/Sieburgh 6-IV 2019.

A.S. Hartkamp & C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Wolters Kluwer 2019.

Hartlief e.a., 2018.

T. Hartlief, A.L.M. Keirse, S.D. Lindenbergh en R.D. Vriesendorp, *Verbintenissen uit de wet en schadevergoeding*, Deventer: Wolters Kluwer 2018.

Hijmans, 2018.

H. Hijmans, ‘*De AVG en de UAVG’*, NJB 2018/356, afl. 7.

Van der Hof, e.a., 2014.

S. van der Hof, A.R. Lodder, G.J. Zwenne, *Recht en computer*, Deventer: Wolters Kluwer 2014.

Hugenholtz, 2012.

P. Hugenholtz, ‘*Gezamenlijke noot bij Scarlet Extended NV/SABAM en SABAM/Netlog NV’*, *NJ* 2012, nrs. 479 en 480.

Ivir, juli 2018.

Ivir, ‘*Global online piracy study’*, juli 2018.

Jagt, 2013.

F. van der Jagt, ‘Grondrechten. De nationale, Europese en internationale dimensie - Het recht op bescherming van persoonsgegevens’, Nijmegen: Ars Aequi Libri 2013.

Kingma, 2012.

S.H. Kingma, ‘De botsing tussen IE-en privacy rechten’, *P&I* 2012, afl. 4.

Van der Kooij, 2019.

P.A.C.E. van der Kooij, *Intellectuele eigendom,* Den Haag: Boom Juridische uitgevers 2019.

Linders & Vermeij, 2019.

Linders en Vermeij, ‘*Dutch FilmWorks / Ziggo: een hoge drempel voor het verkrijgen van NAW-gegevens van individuele downloaders’,* Tijdschrift voor internetrecht 2019, nrs. 3 en 4.

Memorie van toelichting, Gedragscode Notice-and-Take-Down.

Memorie van toelichting, Gedragscode Notice-and-Take-Down.

Music Consumer Insight report 2016, IFPI.

Music Consumer Insight report 2016, IFPI.

Perset, 2010.

K. Perset, “The Economic and Social Role of Internet Intermediaries”, OECD Study, STI/ICCP(2009)9/FINAL, april 2010.

Phillips, 2016

C. Phillips, *Praktisch Goederenrecht*, Groningen: Noordhoff Uitgevers 2016.

Reus 2012.

J. Reus, ‘*De bescherming van IE-rechten op platforms voor user-generated content content – in hoeverre is een maatregel tot preventief filteren mogelijk*?’, IER 2012/5, pag. 413-418.

Sandvine, 2018.

Sandvine, ‘The Global Internet Phenomena’, september 2018.

Schermer en Falot, juni 2014.

B.W. Schermer en N. Falot, ‘*Omdat het gratis is; de schade voor de Nederlandse filmindustrie door downloaden uit illegale bron*’, juni 2014, Amsterdam Considirati.

Schermer, e.a., 2018.

B.W. Schermer, D. Hagenauw en N. Falot, ‘*Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet algemene verordening gegevensbescherming*’, Ministerie van Justitie en Veiligheid, januari 2018.

Van der Sloot, 2018.

B. van der Sloot, *De Algemene Verordening Gegevensbescherming in gewone mensentaal*, Amsterdam: Amsterdam University Press 2018.

Spoor, 1974.

Spoor, WPNR 5254 (1974).

Spoor e.a., 2019.

J.H. Spoor, D.W.F. Verkade en D.J.G. Visser, *Auteursrecht – auteursrecht, naburige rechten en databankenrecht*, Deventer: Wolters Kluwer 2019.

Timmer & Paffen, 2015.

I. Timmer en A.L.A.M. Paffen, Verbintenissenrecht begrepen, Den Haag: Boom Juridische uitgevers 2015.

Visser, 1997.

D.J.G. Visser, *Auteursrecht op toegang*, diss. Leiden. Den Haag 1997, Vuga.

De Vries, 1984.

De Vries, NJB 1984, met naschrift Cohen Jehoram.

Widdershoven, Verhoeven e.a. 2007.

R.J.G.M. Widdershoven, M.J.M. Verhoeven e.a., De Europese agenda van de Awb (derde evaluatie van de Awb), Den Haag: Boom Juridische uitgevers 2007.

**Online**

Autoriteitpersoonsgegevens.nl, zoek op: ‘Algemene verordening gegevensbescherming’.

Autoriteitpersoonsgegevens.nl, ‘hoe weet u of u persoonsgegevens mag verwerken?’.

Autoriteitpersoonsgegevens.nl, ‘verantwoordingsplicht’.

Rechtspraak.nl, ‘*Ziggo hoeft geen inzake te geven in gegevens illegale downloaders’*, 8 februari 2019.

Stichtingbrein.nl, Wat is BREIN?

Stichtingbrein.nl, Aangeslotenen.

**Parlementaire stukken**

Perscommuniqué nr. 37/11, 14 april 2011.

Perscommuniqué nr. 5/08, 29 januari 2008.

*Ministerie van Justitie,* 5536468/08/620 maart 2008.

*Ministerie van Justitie*, Handleiding Algemene Verordening gegevensbescherming, Implementatietabel UAVG.

Vaste Kamercommissie voor Justitie, verzoek van 8 februari 2008 (08-JUST-B-009).

*Kamerstukken II,* 2017/18, 34939 nr. 3 (MvT).

*Kamerstukken II,* 2013/14, nr. 822, Aanhangsel.

*Kamerstukken II*, 2005/06, 30392, nr. 6.

*Kamerstukken II*, 2005/06, 30392, nr. 3 (MvT).

*Kamerstukken II* 2001/02, 28197, nr. 3 (MvT).

**Jurisprudentie**

Hof van Justitie van de Europese Unie 19 april 2012, ECLI:EU:C:2012:219 (*Bonnier Audio/Perfect Communication*).

Hof van Justitie van de Europese Unie 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM).*

Hof van Justitie van de Europese Unie 17 november 2011, ECLI:EU:C:2011:753 (*Conclusie van A-G* *Bonnier Audio/Perfect Communication)*.

Hof van Justitie van de Europese Unie 12 juli 2011, ECLI:EU:C:2011:474 (L’Oréal/eBay).

Hof van Justitie van de Europese Unie 23 maart 2010, ECLI:EU:2010:159 (Google France).

Hof van Justitie van de Europese Unie 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica*).

Hof van Justitie van de Europese Unie 20 mei 2003, ECLI:EU:2003:294 *(Rechnungshof/Osterreichischer Rundfunk).*

Hof van Justitie van de Europese Unie 15 juli 1964, zaak C-6/64 (*Costa/ENEL).*

Hof van Justitie van de Europese Unie 5 februari 1963, zaak C-26/62 (*Van Gend en Loos*).

Hoge Raad 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*).

Hoge Raad 1 juni 1990, NJ 1991/377 m.nt. D.W.F. Verkade (*Kluwer/Lamoth)*.

Hoge Raad 6 mei 1938, NJ 1938/635 (*café radio*).

Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 (*DFW/Ziggo*).

Hof ’s-Hertogenbosch 10 juli 2018, ECLI:NL:GHSHE:2018:2824 (*Newsconnection/BREIN*).

Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (*Ziggo/123 Video*).

Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*).

Rechtbank Oost-Brabant 12 maart 2019, ECLI:NL:RBOBR:2019:1286.

Rechtbank Midden-Nederland 8 februari 2019, ECLI:NL:RBMNE:2019:423 (*DFW/Ziggo*).

Rechtbank Amsterdam 21 december 2018, ECLI:NL:RBAMS:2018:9362 (*Tommy Hilfiger/Facebook).*

Rechtbank Noord-Holland 7 juni 2017, ECLI:RBNHO:2017:4435 (*BREIN/Eweka*).

Rechtbank Amsterdam 26 april 2017, ECLI:NLRBAMS:2017:4038 (*XS News/Abavia).*

Rechtbank Oost-Brabant 12 december 2016, ECLI:NL:RBOBR:2016:6846 (*BREIN/Newsconnection*).

Rechtbank Limburg 24 november 2016, ECLI:NL:RBLIM:2016:9210 (*X/Vodafone)*.

Rechtbank Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*).

RechtbankRotterdam 20 juli 2016, ECLI:NL:RBROT:2016:7505.

Rechtbank Noord-Holland 23 juni 2016, ECLI:NL:RBNHO:2016:4893 (*BREIN/Eweka*).

RechtbankMidden-Nederland 16 december 2015, ECLI:NL:RBMNE:2015:8974 *(Stichting BREIN/Ziggo).*

Rechtbank Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*).

RechtbankAmsterdam 9 oktober 2008, ECLI:NL:RBAMS:2008:BF7448 *(GOOGLE).*

Rechtbank Den Bosch 8 juli 2008, IEPT 20080709 (*BREIN/Euroaccess).*

Rechtbank Den Haag 5 januari 2007, ECLI:NL:RBSGR:2007:AZ5678 (*BREIN/KPN*).

Rechtbank Amsterdam 24 augustus 2006, ECLI:NLRBAMS:2006:AY6903 (*BREIN/UPC*).

Rechtbank Noord-Holland 5 juli 2006, ECLI:NL:RBNHO:2016:5535 *(Instagram).*

Rechtbank. Utrecht 12 juli 2005, ECLI:NL:RBUTR:2005:AT9073 (*BREIN/ vijf internetproviders).*

# Bijlage

*Jurisprudentieonderzoek*

1. Ivir, juli 2018. [↑](#footnote-ref-1)
2. Sandvine 2018. [↑](#footnote-ref-2)
3. Schermer en Falot, juni 2014. [↑](#footnote-ref-3)
4. Radar Avrotros, augustus 2016. [↑](#footnote-ref-4)
5. Music Consumer Insight report 2016, IFPI. [↑](#footnote-ref-5)
6. Stichtingbrein.nl, Wat is BREIN? [↑](#footnote-ref-6)
7. HR 1 juni 1990, NJ 1991/377 (*Kluwer/Lamoth).* [↑](#footnote-ref-7)
8. Van der Kooij, 2019, pag. 20. [↑](#footnote-ref-8)
9. Gielen, e.a., 2018, pag. 465. [↑](#footnote-ref-9)
10. Gielen, e.a., 2018, pag. 541. [↑](#footnote-ref-10)
11. Stichtingbrein.nl, Aangeslotenen. [↑](#footnote-ref-11)
12. Art. 6:162 lid 2 BW. [↑](#footnote-ref-12)
13. Timmer & Paffen, 2015, pag. 213. [↑](#footnote-ref-13)
14. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-14)
15. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-15)
16. Van der Hof, e.a., 2014, pag. 270. [↑](#footnote-ref-16)
17. Gielen, e.a., 2018, pag. 603. [↑](#footnote-ref-17)
18. HvJ 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica)*. [↑](#footnote-ref-18)
19. HvJ 19 april 2012, ECLI:EU:C:2012:219 (*Bonnier Audio/Perfect Communication*). [↑](#footnote-ref-19)
20. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-20)
21. Autoriteitspersoonsgegevens.nl, Algemene verordening gegevensbescherming. [↑](#footnote-ref-21)
22. Schermer, e.a., 2018, pag. 36 [↑](#footnote-ref-22)
23. Autoriteitpersoonsgegevens.nl “hoe weet u of u persoonsgegevens mag verwerken?”. [↑](#footnote-ref-23)
24. Rechtspraak.nl, 8 februari 2019. [↑](#footnote-ref-24)
25. Linders & Vermeij, 2019, pag. 127-130. [↑](#footnote-ref-25)
26. Rb. Midden-Nederland 8 februari 2019, ECLI:NL:RBMNE:2019:423 (*DFW/Ziggo*). [↑](#footnote-ref-26)
27. Protocol, 6 juli 2017. [↑](#footnote-ref-27)
28. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 (*DFW/Ziggo)*. [↑](#footnote-ref-28)
29. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-29)
30. HvJ EU 5 februari 1963, zaak C-26/62 (*Van Gend en Loos*) en HvJ EU 15 juli 1964, zaak C-6/64 (*Costa/ENEL).* [↑](#footnote-ref-30)
31. Alberdingk Thijm en De Vries, BIE 2015, pag. 174-183. [↑](#footnote-ref-31)
32. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-32)
33. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-33)
34. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-34)
35. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-35)
36. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-36)
37. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-37)
38. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-38)
39. Stichtingbrein.nl, Aangeslotenen. [↑](#footnote-ref-39)
40. Spoor e.a., 2019, pag. 487. [↑](#footnote-ref-40)
41. Gielen, e.a., 2018, pag. 572. [↑](#footnote-ref-41)
42. Perset, 2010, pag. 9. [↑](#footnote-ref-42)
43. *Kamerstukken II,* 2001/02, 28197, nr. 3, p. 46-51 (MvT). [↑](#footnote-ref-43)
44. HvJ EU 23 maart 2010, ECLI:EU:2010:159 (Google France), r.o. 114 en 120. HvJ EU 12 juli 2011, ECLI:EU:C:2011:474 (L’Oréal/eBay), r.o. 113 en 119. [↑](#footnote-ref-44)
45. Reus 2012, pag. 415. [↑](#footnote-ref-45)
46. *Kamerstukken II,* 2001/02, 28197, nr. 3, pag. 49 (MvT). [↑](#footnote-ref-46)
47. Gielen, e.a., 2018, pag. 572. [↑](#footnote-ref-47)
48. Memorie van toelichting Gedragscode Notice-and-Take-Down. [↑](#footnote-ref-48)
49. *Kamerstukken II,* 2001-02, 28197, nr. 3, pag. 50-51 (MvT). [↑](#footnote-ref-49)
50. Spoor e.a., 2019, pag. 14. [↑](#footnote-ref-50)
51. De Vries, *NJB* 1984, pag. 15. [↑](#footnote-ref-51)
52. Brinkhof, *NJB* 1994, pag. 771. [↑](#footnote-ref-52)
53. Van der Kooij, 2019, pag. 25. [↑](#footnote-ref-53)
54. Gielen, e.a., 2018, pag. 465. [↑](#footnote-ref-54)
55. Spoor e.a., 2019, pag. 2. [↑](#footnote-ref-55)
56. Spoor e.a., 2019, pag. 177. [↑](#footnote-ref-56)
57. Gielen, e.a., 2018, pag 519. [↑](#footnote-ref-57)
58. Geerts, 2019, pag. 69-70. [↑](#footnote-ref-58)
59. HR 6 mei 1938, NJ 1938/635 (*café radio*). [↑](#footnote-ref-59)
60. Spoor, 1974, pag. 165. [↑](#footnote-ref-60)
61. Spoor e.a., 2019, pag. 151. [↑](#footnote-ref-61)
62. Geerts, 2019, pag. 64-65. [↑](#footnote-ref-62)
63. Spoor e.a., 2019, pag. 151. [↑](#footnote-ref-63)
64. Geerts, 2018, pag. 64-65. [↑](#footnote-ref-64)
65. Gielen, e.a., 2019, pag 509-510. [↑](#footnote-ref-65)
66. *Kamerstukken II,* 2013/14, nr. 822, Aanhangsel. [↑](#footnote-ref-66)
67. Spoor e.a., 2019, pag. 9. [↑](#footnote-ref-67)
68. Dijkstra, 2008, pag. 136. [↑](#footnote-ref-68)
69. Visser, 1997, pag. 146-179. [↑](#footnote-ref-69)
70. Spoor e.a., 2019, pag. 9. [↑](#footnote-ref-70)
71. Bauch, e.a., 1999, pag. 27. [↑](#footnote-ref-71)
72. Spoor e.a., 2019, pag. 9-10. [↑](#footnote-ref-72)
73. Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten. [↑](#footnote-ref-73)
74. Overweging 10 van de Handhavingsrichtlijn. [↑](#footnote-ref-74)
75. Overweging 21 van de Handhavingsrichtlijn. [↑](#footnote-ref-75)
76. Gielen, e.a., 2018, pag. 603. [↑](#footnote-ref-76)
77. Kamerstukken II, 2005/06, 30392, nr. 3, pag. 7 (MvT). [↑](#footnote-ref-77)
78. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-78)
79. Dijkstra, 2008, pag. 136. [↑](#footnote-ref-79)
80. Rb. Oost-Brabant 12 maart 2019, ECLI:NL:RBOBR:2019:1286. [↑](#footnote-ref-80)
81. Gellaerts & Jobse, 2019, pag. 203. [↑](#footnote-ref-81)
82. Van der Hof, e.a., 2014, pag. 272. [↑](#footnote-ref-82)
83. Gielen, e.a., 2018, pag. 541. [↑](#footnote-ref-83)
84. Spoor e.a., 2019, pag. 523-525. [↑](#footnote-ref-84)
85. *Kamerstukken II*, 2005/06, 30392, nr. 6, pag. 2-3. [↑](#footnote-ref-85)
86. Asser/Sieburgh 6-IV 2019/36. [↑](#footnote-ref-86)
87. Asser/Sieburgh 6-IV 2019/43. [↑](#footnote-ref-87)
88. Hartlief e.a., 2018, pag. 37-38. [↑](#footnote-ref-88)
89. Van der Kooij, 2019, pag. 11. [↑](#footnote-ref-89)
90. Phillips, 2016, pag. 29 [↑](#footnote-ref-90)
91. Asser/Sieburgh 6-IV 2019/30. [↑](#footnote-ref-91)
92. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-92)
93. Rb. Noord-Holland 5 juli 2006, ECLI:NL:RBNHO:2016:5535 (*Instagram*), Rb. Midden-Nederland 16 december 2015, ECLI:NL:RBMNE:2015:8974 (*Stichting BREIN/Ziggo*), Rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:7505 en Rb. Amsterdam 9 oktober 2008, ECLI:NL:RBAMS:2008:BF7448 (*GOOGLE*). [↑](#footnote-ref-93)
94. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-94)
95. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-95)
96. Implementatietabel UAVG, Handleiding Algemene Verordening gegevensbescherming. [↑](#footnote-ref-96)
97. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-97)
98. Van der Hof, e.a., 2014, pag. 270. [↑](#footnote-ref-98)
99. Jagt, 2013, pag. 163-164. [↑](#footnote-ref-99)
100. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM).* [↑](#footnote-ref-100)
101. Hugenholtz, 2012, pag. 5395-5397. [↑](#footnote-ref-101)
102. Jagt, 2013, pag. 163-164. [↑](#footnote-ref-102)
103. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM).* [↑](#footnote-ref-103)
104. Perscommuniqué nr. 37/11, 14 april 2011. [↑](#footnote-ref-104)
105. Hugenholtz, 2012, pag. 5395-5397. [↑](#footnote-ref-105)
106. Chavannes, AMI 2015/2, pag. 43. [↑](#footnote-ref-106)
107. Jagt, 2013, pag. 163-164. [↑](#footnote-ref-107)
108. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM), r.o. 48.* [↑](#footnote-ref-108)
109. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM), r.o. 49.* [↑](#footnote-ref-109)
110. Verordening (EU) 95/25/EG. [↑](#footnote-ref-110)
111. Engelfriet, e.a., 2019, pag. 13. [↑](#footnote-ref-111)
112. *Kamerstukken II, 2017/18*, 34939 nr. 3 pag. 1 (MvT). [↑](#footnote-ref-112)
113. Hijmans, 2018, pag. 472. [↑](#footnote-ref-113)
114. Verordening (EU) 2016/679, overweging 6-7, pag. 2. [↑](#footnote-ref-114)
115. Van der Sloot, 2018, pag. 22-24. [↑](#footnote-ref-115)
116. Engelfriet, e.a., 2019, pag. 13. [↑](#footnote-ref-116)
117. Berkvens & Jakimowics, 2018, pag. 665-682. [↑](#footnote-ref-117)
118. *Kamerstukken II, 2017/18*, 34939 nr. 3 pag. 4 (MvT). [↑](#footnote-ref-118)
119. Schermer, e.a., 2018, pag. 21-22. [↑](#footnote-ref-119)
120. HvJ EU 20 mei 2003, ECLI:EU:2003:294 *(Rechnungshof/Osterreichischer Rundfunk).* [↑](#footnote-ref-120)
121. Engelfriet, e.a., 2019, pag. 39. [↑](#footnote-ref-121)
122. Schermer, e.a., 2018, pag. 36-40. [↑](#footnote-ref-122)
123. Autoriteitpersoonsgegevens.nl “hoe weet u of u persoonsgegevens mag verwerken?”. [↑](#footnote-ref-123)
124. Engelfriet, e.a., 2019, pag. 115-116. [↑](#footnote-ref-124)
125. Van der Sloot, 2018, pag. 89. [↑](#footnote-ref-125)
126. Autoriteitpersoonsgegevens.nl/ “verantwoordingsplicht”. [↑](#footnote-ref-126)
127. Engelfriet, e.a. 2019, pag. 119. [↑](#footnote-ref-127)
128. Rb. Midden-Nederland 8 februari 2019, ECLI:NL:RBMNE:2019:423 (*DFW/Ziggo).* [↑](#footnote-ref-128)
129. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 (*DFW/Ziggo).* [↑](#footnote-ref-129)
130. Rb. Amsterdam 21 december 2018, ECLI:NL:RBAMS:2018:9362 (*Tommy Hilfiger/Facebook).* [↑](#footnote-ref-130)
131. Engelfriet, e.a., 2019, pag. 103. [↑](#footnote-ref-131)
132. Verordening (EU) 2016/679, overweging 70, pag. 13. [↑](#footnote-ref-132)
133. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-133)
134. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-134)
135. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-135)
136. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-136)
137. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-137)
138. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-138)
139. Kingma,2012, pag. 172-176. [↑](#footnote-ref-139)
140. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-140)
141. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-141)
142. Kingma,2012, pag. 172. [↑](#footnote-ref-142)
143. HvJ EU 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica).* [↑](#footnote-ref-143)
144. Dommering, 2011, pag. 49-53. [↑](#footnote-ref-144)
145. Perscommuniqué nr. 5/08, 29 januari 2008. [↑](#footnote-ref-145)
146. HvJ EU 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica).* [↑](#footnote-ref-146)
147. HvJ EU 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica).* [↑](#footnote-ref-147)
148. HvJ EU 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica).* [↑](#footnote-ref-148)
149. Kingma,2012, pag. 173. [↑](#footnote-ref-149)
150. HvJ EU 29 januari 2008, ECLI:EU:C:2008:54 (*Promusicae/Telefónica)*. [↑](#footnote-ref-150)
151. Ministerie van Justitie, 5536468/08/6 20 maart 2008. [↑](#footnote-ref-151)
152. Vaste Kamercommissie voor Justitie, verzoek van 8 februari 2008. [↑](#footnote-ref-152)
153. Ministerie van Justitie, 5536468/08/6 20 maart 2008. [↑](#footnote-ref-153)
154. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-154)
155. Ministerie van Justitie, 5536468/08/6 20 maart 2008. [↑](#footnote-ref-155)
156. HvJ EU 19 april 2012, ECLI:EU:C:2012:219 (*Bonnier Audio/Perfect Communication*). [↑](#footnote-ref-156)
157. HvJ EU 19 april 2012, ECLI:EU:C:2012:219 (*Bonnier Audio/Perfect Communication*). [↑](#footnote-ref-157)
158. HvJ EU 19 april 2012, ECLI:EU:C:2012:219 (*Bonnier Audio/Perfect Communication*). [↑](#footnote-ref-158)
159. Kingma, 2012, pag. 173. [↑](#footnote-ref-159)
160. Ministerie van Justitie, 5536468/08/6 20 maart 2008. [↑](#footnote-ref-160)
161. Rb. Limburg 24 november 2016, ECLI:NL:RBLIM:2016:9210 (*X/Vodafone)*. [↑](#footnote-ref-161)
162. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-162)
163. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-163)
164. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-164)
165. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-165)
166. Deze vier criteria zijn uitgewerkt in paragraaf 2.8. [↑](#footnote-ref-166)
167. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM).* [↑](#footnote-ref-167)
168. Perscommuniqué nr. 37/11, 14 april 2011. [↑](#footnote-ref-168)
169. EU HvJ 24 november 2011, ECLI:EU:C:2011:771 (*Scarlet Extended/SABAM).* [↑](#footnote-ref-169)
170. Jagt, 2013, pag. 163-164. [↑](#footnote-ref-170)
171. Rb. Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*). [↑](#footnote-ref-171)
172. Rb. Den Haag 5 januari 2007, ECLI:NL:RBSGR:2007:AZ5678 (*BREIN/KPN*). [↑](#footnote-ref-172)
173. Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (*Ziggo/123 Video*) en Rb. Amsterdam 26 april 2017, ECLI:NLRBAMS:2017:4038 (*XS News/Abavia).* [↑](#footnote-ref-173)
174. Rb. Amsterdam 26 april 2017, ECLI:NLRBAMS:2017:4038 (*XS News/Abavia).* [↑](#footnote-ref-174)
175. De doelstelling van BREIN is verder besproken in paragraaf 2.1. [↑](#footnote-ref-175)
176. Dit is behandeld in paragraaf 2.9. [↑](#footnote-ref-176)
177. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 *(DFW/Ziggo).* [↑](#footnote-ref-177)
178. Rb. Oost-Brabant 12 december 2016, ECLI:NL:RBOBR:2016:6846 (*BREIN/Newsconnection*). [↑](#footnote-ref-178)
179. Rb. Amsterdam 24 augustus 2006, ECLI:NL:RBAMS:2006:AY6903 (*BREIN/UPC*), Rb. Utrecht 12 juli 2005, ECLI:NL:RBUTR:2005:AT9073 (*BREIN/ vijf internetproviders)* enRb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-179)
180. Rb. Amsterdam 24 augustus 2006, ECLI:NL:RBAMS:2006:AY6903 (*BREIN/UPC*). [↑](#footnote-ref-180)
181. Rb. Amsterdam 24 augustus 2006, ECLI:NL:RBAMS:2006:AY6903 (*BREIN/UPC*) r.o. 9. [↑](#footnote-ref-181)
182. Rb. Amsterdam 24 augustus 2006, ECLI:NL:RBAMS:2006:AY6903 (*BREIN/UPC*). [↑](#footnote-ref-182)
183. Hof ’s-Hertogenbosch 10 juli 2018, ECLI:NL:GHSHE:2018:2824 (*Newsconnection/BREIN*). [↑](#footnote-ref-183)
184. Hof ’s-Hertogenbosch 10 juli 2018, ECLI:NL:GHSHE:2018:2824 (*Newsconnection/BREIN*) r.o. 2.11.2. [↑](#footnote-ref-184)
185. Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*). [↑](#footnote-ref-185)
186. Rb. Noord-Holland 23 juni 2016, ECLI:NL:RBNHO:2016:4893 (*BREIN/Eweka*). [↑](#footnote-ref-186)
187. Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*), IEPT 20080708 (*BREIN/Euroaccess*) en Rb. Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*). [↑](#footnote-ref-187)
188. Hof Amsterdam 3 juli 2008, ECLI:NL:GHAMS:2008:BD6223 (*Leaseweb/BREIN*). [↑](#footnote-ref-188)
189. Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-189)
190. Rb. Noord-Holland 23 juni 2016, ECLI:NL:RBNHO:2016:4893 (*BREIN/Eweka*) en Rb. Oost-Brabant 12 december 2016, ECLI:NL:RBOBR:2016:6846 (*BREIN/Newsconnection*). [↑](#footnote-ref-190)
191. Rb. Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*), Rb. Den Bosch 8 juli 2008, IEPT 20080708 (*BREIN/Euroacces*) en Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-191)
192. Rb. Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*). [↑](#footnote-ref-192)
193. Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (*Ziggo/123 Video*). [↑](#footnote-ref-193)
194. Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-194)
195. Rb. Noord-Holland 22 juni 2016, ECLI:NL:RBNHO:2016:4893 (*BREIN/Eweka*). [↑](#footnote-ref-195)
196. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-196)
197. Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-197)
198. Rb. Noord-Holland 22 juni 2016, ECLI:NL:RBNHO:2016:4893 (*BREIN/Eweka*). [↑](#footnote-ref-198)
199. Rb. Noord-Holland 7 juni 2017, ECLI:RBNHO:2017:4435 (*BREIN/Eweka*). [↑](#footnote-ref-199)
200. Rb. Utrecht 12 juli 2005, ECLI:NL:RBUTR:2005:AT9073 (*BREIN/ vijf internetproviders).* [↑](#footnote-ref-200)
201. Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BP7309 (*Ziggo/123 Video*). [↑](#footnote-ref-201)
202. Rb. Midden-Nederland 8 februari 2019, ECLI:NLRBMNE:2019:423 (*DFW/Ziggo*). [↑](#footnote-ref-202)
203. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 *(DFW/Ziggo).* [↑](#footnote-ref-203)
204. Widdershoven, Verhoeven e.a. 2007, pag. 35. [↑](#footnote-ref-204)
205. Jagt, 2013, pag. 163-164. [↑](#footnote-ref-205)
206. Rb. Den Haag 24 oktober 2012, IEPT 20121024 (*BREIN/XS Networks*). [↑](#footnote-ref-206)
207. Rb. Den Haag 17 augustus 2016, ECLI:NL:RBDHA:2016:9685 (*Eredivisie/Global Layer*). [↑](#footnote-ref-207)
208. Rb. Noord-Holland 7 juni 2017, ECLI:RBNHO:2017:4435 (*BREIN/Eweka*). [↑](#footnote-ref-208)
209. Hof ’s-Hertogenbosch 10 juli 2018, ECLI:NL:GHSHE:2018:2824 (*Newsconnection/BREIN)*. [↑](#footnote-ref-209)
210. Rb. Amsterdam 21 december 2018, ECLI:NL:RBAMS:2018:9362 (*Tommy Hilfiger/Facebook*). [↑](#footnote-ref-210)
211. Rb. Midden-Nederland 8 februari 2019, ECLI:NLRBMNE:2019:423 (*DFW/Ziggo*). [↑](#footnote-ref-211)
212. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 *(DFW/Ziggo).* [↑](#footnote-ref-212)
213. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-213)
214. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-214)
215. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-215)
216. Rb. Midden-Nederland 8 februari 2019, ECLI:NL:RBMNE:2019:423 (*DFW/Ziggo).* [↑](#footnote-ref-216)
217. Hof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352 (*DFW/Ziggo).* [↑](#footnote-ref-217)
218. Rb. Amsterdam 21 december 2018, ECLI:NL:RBAMS:2018:9362 (*Tommy Hilfiger/Facebook*). [↑](#footnote-ref-218)
219. HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). [↑](#footnote-ref-219)