Op weg naar evenwicht

Een onderzoek naar zorgplichten op het internet

Instituut voor Informatierecht (IViR)

Leibniz Center for Law

Prof. Dr. N.A.N.M. van Eijk
Prof. Dr. T.M. van Engers

Mr. C. Wiersma
Mr. C.A. Jasserand
Mr. W. Abel

Universiteit van Amsterdam

2010

Op weg naar evenwicht

Een onderzoek naar zorgplichten op het internet

Instituut voor Informatierecht (IViR)
Leibniz Center for Law

Prof. Dr. N.A.N.M. van Eijk
Prof. Dr. T.M. van Engers

Mr. C. Wiersma
Mr. C.A. Jasserand
Mr. W. Abel

Universiteit van Amsterdam
2010

Inhoudsopgave

Samenvatting

In opdracht van het WODC is onderzoek verricht naar zorgplichten op het internet, meer in het bijzonder vanuit het perspectief van internetserviceproviders. Internetserviceproviders staan zowel op nationaal als internationaal volop in de belangstelling, niet alleen voor wat betreft hun verhouding tot de overheid, maar ook ten opzichte van andere privaatrechtelijke partijen, bijvoorbeeld met betrekking tot (civielrechtelijke) aansprakelijkheid. Dit onderzoek richt zich op de eerste relatie, zorgplichten in de relatie tussen overheid en internetserviceproviders. Waar deze ontbreekt is wel nagegaan of er mogelijk elders in de waardeketen tussen informatiediensten aanbieders en eindgebruikers waarvan internetserviceproviders deel uitmaken zorgplichten spelen.

De situatie in vier landen - Nederland, Verenigd Koninkrijk, Duitsland en Frankrijk - is onderzocht. De (zelf)regulering met betrekking tot een vijftal thema's is in kaart gebracht (internetveiligheid, kinderporno, auteursrechten, identiteitsfraude en de handel in gestolen goederen via internetplatforms). Daarnaast is een groot aantal interviews gehouden met betrokken partijen.

Uit het onderzoek komt een wisselend beeld naar voren, wat erop duidt dat ontwikkelingen nog volop in gang zijn. Internetveiligheid, meer in het bijzonder voor zover het de relatie tussen de internetserviceprovider en de eindgebruiker betreft, staat duidelijk nog in de kinderschoenen. Dit betekent niet dat er in de praktijk niets gebeurt, maar er is nog weinig formele inkadering of zelfregulering. Kinderporno daarentegen kent een vrijwel identiek regime in de onderzochte landen, waarbij partijen bereid zijn om vergaande medewerking te verlenen bij de bestrijding ervan. Een meldsysteem voor kinderporno is in alle landen aanwezig op basis van zelfregulering of als uitvloeisel van een wettelijk gedefinieerde zorgverplichting. Terugkerend issue bij het tegengaan van de verspreiding van kinderporno is de positie van filtering en blokkering. Auteursrecht krijgt veel aandacht en heeft in twee van de onderzochte landen tot aanscherping van de regelgeving geleid, waardoor het mogelijk is om eindgebruikers af te sluiten van internettoegang of deze toegang te beperken. De kritiek op de nieuwe regels is echter groot en de interviews geven aan dat men zeer kritisch is wat betreft de daadwerkelijke handhavingsmogelijkheden. Identiteitsfraude wordt vooral aangepakt in de context van de gevolgen van identiteitsfraude. Het zelfstandig strafbaar stellen van identiteitsfraude (naast de al bestaande mogelijkheden om in de publiekrechtelijke sfeer handhavend op te treden) wordt veelal niet noodzakelijk geacht. De verkoop van gestolen goederen via platform aanbieders (lees: veiling- en verkoopsites e.d.) wordt gezien als de primaire verantwoordelijkheid van de platformaanbieder.

Het wisselende beeld, de nog volop aanwezige dynamiek, het zoeken naar meer evenwicht in de verhoudingen, brengt met zich mee dat het niet mogelijk is om bijvoorbeeld bewezen 'best practices' vast te stellen. Dit betekent dat er enerzijds nog veel onzekerheid is,

anderzijds ligt hierin een uitdaging voor verdere beleidsvorming. Desalniettemin bieden de in het onderzoek verzamelde gegevens interessante informatie.
De onderzoekers komen op grond van het door hen gedane onderzoek tot de volgende conclusies:

1. Naar een waardeketen-benadering
Zorgplichten, voor zover in het onderzoek geanalyseerd, kunnen niet gekoppeld worden aan één specifieke partij in de waardeketen tussen informatiedienstenaanbieders en eindgebruikers, maar dienen een gezamenlijke - gebalanceerde - verantwoordelijkheid te zijn van de betrokkenen in de waardeketen waartoe naast internetserviceproviders ook partijen behoren zoals aanbieders van informatiediensten, platforms, zoekmachines en hosting diensten.

2. Ex ante toetsing effectiviteit en handhaafbaarheid
Vooraf toetsing van (beoogde) juridische interventie met betrekking tot effectiviteit en handhaafbaarheid draagt bij aan het voorkomen van symboolwetgeving en ongewenste effecten.

3. Inzetbaarheid 'notice and take down' -procedures
'Notice and take down'-procedures blijken een breed geaccepteerd mechanisme. De procedures worden niet alleen gehanteerd door internetserviceproviders (in hun hoedanigheid als aanbieder van hosting en caching diensten). Ook andere partijen in de waardeketen, zoals platform-aanbieders, kennen vergelijkbare procedures. Een specifieke juridische grondslag ontbreekt evenwel in de meeste onderzochte landen. Wel zijn er initiatieven in de sfeer van zelf- en coregulering. Aanbevolen wordt om 'notice and take down'-procedures verder in te kaderen, bijvoorbeeld door een nadere juridische inbedding.

4. Internetveiligheid en privacy verduidelijken
De nieuwe regels inzake internetveiligheid en privacy (artikel 4 van de Europese richtlijn inzake Privacy en de elektronische communicatie) zijn onduidelijk en vragen verdere precisering wat betreft betekenis en impact. Hier ligt mede een taak op Europees niveau ten einde te voorkomen dat er te grote verschillen op nationaal niveau optreden.

5. Verhoging kennisniveau
De behoefte tot nadere regulering wordt mede gevoed door het ontbreken van voldoende technische en praktische kennis. Kennislacunes blijken breed aanwezig te zijn. Wanneer eindgebruikers, toezichthouders, handhavers en regelgevers hun kennis verder vergroten zal dit kunnen bijdragen aan een verminderde reguleringsdruk. Het belang van educatie wordt breed gedragen.

Woord vooraf

In opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC, Ministerie van Justitie) hebben het Instituut voor Informatierecht (IViR) en het Leibniz Center for Law (Leibniz) onderzoek verricht naar zorgplichten op het internet. Het onderzoek is uitgevoerd door Prof. dr. Nico van Eijk (IViR) en Prof. dr. Tom van Engers (Leibniz), in samenwerking met mr. Wiebke Abel, mr. Catherine Jasserand en mr. Chris Wiersma.

Zorgplichten zien in het kader van dit onderzoek op de relatie tussen overheden en internetserviceproviders. Deze kunnen zijn vastgelegd in de vorm van wetgeving of nadere regelgeving. Maar zorgplichten kunnen ook tot uitdrukking komen in vormen van co/zelfregulering.

Bij het bestuderen van relevante zorgplichten is de positie van de internetserviceprovider als uitgangspunt genomen. De rol van de internetserviceprovider staat echter niet op zichzelf, maar maakt onderdeel uit van een bredere waardeketen tussen aanbieders van informatiediensten en eindgebruikers.

Het onderzoek is gedaan in vier landen (Nederland, Frankrijk, Duitsland, Verenigd Koninkrijk) aan de hand van een vijftal thema's (internetveiligheid, kinderporno, auteursrechten, identiteitsfraude, verkoop van gestolen goederen) en kent zowel een kwantitatieve als kwalitatieve benadering. De (zelf)regulering met betrekking tot zorgplichten is geïnventariseerd en beschreven. Om een zo accuraat mogelijk beeld te krijgen van de situatie in de onderzochte landen zijn interviews gehouden met de belangrijkste betrokkenen.

De onderzoekers danken met name de geïnterviewden die bereid zijn geweest om ruimhartig tijd vrij te maken voor vaak zeer informatieve en openhartige gesprekken.

Amsterdam, juni 2010

Afkortingen

AFA	Association des Fournisseurs d´Accès et de Services Internet
AFOM	Association Française des Opérateurs Mobiles
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARCEP	Autorité de régulation des communicatons électroniques et des postes
BEFTI	La Brigade d'enquêtes sur les fraudes aux technologies de l'information
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BVerfG	Bundesverfassungsgericht
BW	Burgerlijk Wetboek
CIRCAMP	Cospol Internet Related Child Abusive Material Project (www.circamp.eu)
CNIL	Commission nationale de l'informatiques et des libertés
CP	Code Pénal
CPCE	Code des postes et des communications électroniques
CPI	Code de la Propriété Intellectuelle
CPP	Code de Procédure Pénale
CSPLA	Conseil Supérieur de la Propriété Littéraire et Artistique
DADVSI	Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information
DNS	Domain Name System
ECO	Electronic Commerce Forum (Verband der deutschen Internetwirtschaft e.V.)
ECP-EPN	ECP-EPN | Platform voor de InformatieSamenleving, (www.ecp.nl)
FCACP	Financial Coalition Against Child Pornography
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet
INHOPE	International Association of Internet Hotlines
ISPA UK	Internet Services Providers' Association United Kingdom
IWF	Internet Watch Foundation
KLPD	Korps landelijke politiediensten
LCEN	Loi pour la confiance dans l'économie numérique

Loi HADOPI	Loi favorisant la diffusion et la protection de la création sur internet.
Loi HADOPI 2	Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet
Loi Informatique et Libertés	Loi relative à l'informatique, aux fichiers et aux libertés
LOPPSI II	Loi d'Orientation et de Programmation pour la Sécurité Intérieure
NICC	Nederlandse Infrastructuur ter bestrijding van Cybercrime
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.
OFCOM	Office of Communications
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PHAROS	Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements
SOCA	Serious Organised Crime Agency
Sr	Wetboek van Strafrecht
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
Sv	Wetboek van Strafvordering
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Tw	Telecommunicatiewet
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
VeRO	Verified Right Owner Program
Wbp	Wet bescherming persoonsgegevens
ZugErschwG	Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen

Verklarende Woordenlijst

Botnet	Term voor een verzameling van software robots die autonoom en automatisch opereren. De term wordt meestal geassocieerd met kwaadaardige software: botnets zijn dan ook netwerken van besmette computers, die ook 'zombie' PC's worden genoemd.
Caching	De tijdelijke, maar ongewijzigde opslag van informatie, bijvoorbeeld bij de verwerking van internetverkeer.
Deep Packet Inspection	Een methode om te kijken in de datapakketjes die via het internet worden verstuurd.
(Draadloze) router	Randapparaat dat (inkomende en uitgaande) signalen van en naar een telefoonverbinding converteert en verzend ten behoeve van een (draadloze) internetverbinding van een computer.
Finger printing	Het nemen van een 'vingerafdruk', bijvoorbeeld van een muziekbestand dat resulteert in een zogenaamde soundfile waarmee oorspronkelijk bestanden zijn te herkennen.
Grooming	Het online contact zoeken met kinderen met de bedoeling hen online en/of offline seksueel te misbruiken.
Hosting/webhosting	dienst die particulieren of bedrijven ruimte aanbiedt voor het opslaan van informatie, afbeeldingen, of andere inhoud die toegankelijk is via een website.
Internetserviceprovider	Marktpartijen die zich bezig houden met het aan eindgebruikers verschaffen van toegang tot het internet. Deze partijen zijn daarnaast veelal actief als aanbieders van zogenaamde 'hosting' en 'caching'-activiteiten.
Malware	Verzamelnaam voor kwaadaardige en/of schadelijke software. Het woord is een samenvoeging van het Engelse *malicious software* (kwaadwillende software).
Mere conduit	Het onverkort doorgeven/toegang verschaffen tot informatie/het internet.
Notice and take down	Procedure voor het omgaan met meldingen (notice) van inhoud op het internet waarbij na melding een afweging volgt om het materiaal wel of niet van het internet te verwijderen (take down).
Peer to peer	Een computernetwerk waarbij de gebruikers onderling met elkaar zijn verbonden. Er wordt geen gebruik gemaakt van servers.

Phishing	Praktijk waarbij door middel van het kopiëren van bestaande websites een zekere betrouwbaarheid van deze kopieën wordt gefingeerd terwijl het valse websites betreft.
Spam	Ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden.
Virus	Vorm van schadelijke software ('malware'). Het is een computerprogramma dat zich in een bestand kan nestelen, bijvoorbeeld in bestanden van een besturingssysteem.
Zombie PC	Zie 'Botnet'.

1 Inleiding en probleemstelling

1.1 Onderzoeksvraag

Op verzoek van het WODC hebben het Instituut voor Informatierecht (IViR) en het Leibniz Center for Law (Leibniz) onderzoek verricht naar de zorgplicht van internetserviceproviders – die overigens slechts een van de partijen zijn in een complexe waardeketen[1] – in Nederland en een aantal omringende landen. Het onderzoek moet inzicht verschaffen met betrekking tot de vormen van zorgplicht voor internetserviceproviders in Nederland, Frankrijk, Duitsland en het Verenigd Koninkrijk. Daarbij moet ook inzicht worden gegeven in de rol van de nationale overheden en de redenen voor de bestaande inrichtingsvorm. Als centrale onderzoeksvraag is gesteld:

Welke vormen van zorgplicht voor internetserviceproviders gelden in de genoemde landen of worden daar ontwikkeld? Welke rol(len) vervult de nationale overheid daarbij? Wat zijn de redenen voor de gekozen aanpak en wat zijn de ervaringen daarmee?

Bij de centrale onderzoeksvraag is tevens een aantal deelvragen meegegeven, die betrekking hebben op zowel het inventariserende als analyserende deel van het onderzoek (feitelijke/juridische inhoud zorgplichten, ervaringen, (aansturing door) betrokken marktpartijen/overheden, toekomstig beleid/regelgeving). Deze zijn verwerkt in de landenstudies en de beschrijving ervan in hoofdstuk 3.

In het onderzoek worden onder internetserviceproviders verstaan marktpartijen die zich bezig houden met het aan eindgebruikers verschaffen van toegang tot het internet.[2] In telecommunicatierechtelijke termen gaat het om het aanbieden van een 'openbare telecommunicatiedienst'[3]. Deze partijen zijn daarnaast veelal actief als aanbieders van zogenaamde 'hosting' en 'caching'-activiteiten (zie hierna onder 'juridische context').

Bij zorgplichten gaat het primair om de relatie tussen enerzijds de overheid en anderzijds internetserviceproviders. Deze kan tot uitdrukking komen in de vorm van regelgeving of coregulering. Waar dat niet het geval is wordt tevens bezien of er mogelijke vormen van

[1] Zie paragraaf 1.3.

[2] Zie over te hanteren begrippenkaders onder meer OECD(2010), waaraan wij de omschrijving van internetserviceprovider mede ontlenen: '...Internet service providers are generally meant to signify Internet access providers, which provide subscribers with a data connection allowing access to the Internet through physical transport infrastructure.'

[3] Zogenaamde 'resellers' van diensten die door anderen worden aangeboden, vallen in de regel buiten deze definitie.

zelfregulering zijn. Overigens is het vaak moeilijk om een grens te trekken tussen co- en zelfregulering. De relatie overheid-internetserviceproviders kan weer consequenties hebben voor de aansprakelijkheid en verantwoordelijkheid van internetserviceproviders.[4] Deze (civielrechtelijke) aspecten maken geen deel uit van dit onderzoek.

1.2 Thema's

Toetsing van de onderzoeksvraag vindt plaats aan de hand van een vijftal thema's. Deze thema's zijn in overleg met de opdrachtgever gekozen, met als achterliggende gedachte dat zij in beginsel de meest relevante aspecten van de onderliggende problematiek representeren.[5]

In de eerste plaats betreft het inbreuken op internetveiligheid. Op welke wijze is voorzien in een zorgplicht met betrekking tot zaken als privacy-inbreuken of het plaatsen van malware? Internetveiligheid is al onderwerp van regulering op grond van het Europese kader voor de communicatiesector. Dit perspectief, zoals vervat in artikel 4 van de Richtlijn Privacy en elektronische communicatie, is leidend bij het onderzoek.

Tweede onderwerp betreft kinderporno. Kinderporno en internet behoort tot de onderwerpen die al in een vroeg stadium aandacht hebben gevraagd en waarbij er betrokkenheid is van internetserviceproviders.

Auteursrechten is het derde thema van het onderzoek. De aandacht gaat niet uit naar het auteursrecht als zodanig, maar de vraagstelling richt zich op de mogelijke betrokkenheid van de internetserviceprovider bij het eerbiedigen en handhaven van geldende auteursrechten.

Identiteitsfraude is als vierde thema opgenomen. De reden voor dit thema is met name gelegen in het feit dat in 2007 door de Europese Commissie is geadviseerd om van identiteitsfraude een zelfstandig misdrijf te maken.

Als laatste thema is gekeken naar de vraag of internetserviceproviders een rol spelen bij de verkoop van gestolen goederen, meer in het bijzonder wanneer het gaat om het aanbieden van dergelijke goederen via een platform zoals een veilingsite.

Op onderdelen overlappen de thema's elkaar c.q. doet zich vergelijkbare problematiek voor. Dit is bijvoorbeeld het geval met veiligheidsaspecten, toegepaste procedures (zoals vormen van notice and take down[6]) of op het gebied van de handhaving.

---

[4] Zie over aansprakelijkheidsvragen onder meer: De Cock Buning & Van Eek (2009); Van Hoboken (2009).
[5] Voor een bredere beschrijving van cybercrime-activiteiten zie: Van der Hulst/Neve (2008).
[6] Zie over notice and take down paragraaf 1.4.2

In het onderzoek worden de thema's niet uitputtend behandeld, maar vooral bezien vanuit de centrale onderzoeksvraag, namelijk of en zo ja, hoe ten aanzien van deze thema's een geregelde relatie bestaat tussen overheid en internetserviceproviders.

1.3 Waardeketen

Internetserviceproviders zijn slechts een van de partijen die actief zijn in de waardeketen tussen eindgebruikers en de aanbieders van diensten (diensten van de informatie-maatschappij, maar ook andere vormen van transacties).[7] Een aanbieder van een informatiedienst maakt gebruik van een hosting provider om zijn website toegankelijk te maken op het internet, vervolgens wordt de website ontsloten via intermediairs zoals zoekmachines alvorens eindgebruikers die via een internetserviceprovider internettoegang hebben de informatie op website tot zich nemen. Een ander voorbeeld is de eindgebruiker, die via zijn internetserviceprovider toegang zoekt tot een veiling/verkoopsite en daar goederen aanschaft die weer afkomstig kunnen zijn van een webwinkel die van het betreffende platform gebruik maakt. De transactie wordt afgehandeld via een digitale banktransactie. De waardeketen betreft zo niet alleen aan elkaar gekoppelde handelingen, maar is mede een waardeketen in economische zin met een veelvoud van (financiële) transacties. Daar waar in het onderzoek geen rol voor de internetserviceprovider kon worden vastgesteld, is voor zover mogelijk nagegaan of er wellicht zorgplichten elders in de waardeketen spelen. Juridische inkadering

Voor de beantwoording van de onderzoeksvraag zijn twee juridische kaders leidend, die beide een Europese oorsprong hebben. In de Richtlijn Privacy en elektronische communicatie, die onderdeel uitmaakt van de richtlijnen ter regulering van de communicatiesector, zijn zorgplichten met betrekking tot internetveiligheid opgenomen die voor internetserviceproviders relevant zijn. In de tweede plaats is er de regulering in de E-commerce richtlijn. Ofschoon deze regels over 'mere conduit', 'hosting' en 'caching' zich richten op de aansprakelijkheid van tussenpersonen, zoals internetserviceproviders, blijken zij in veel landen tevens te hebben geresulteerd in zorgplichten/zelfregulering. In de onderzoeksopdracht is nadrukkelijk aandacht gevraagd voor de mededeling van de Europese Commissie waarin identiteitsfraude aan de orde is. Tenslotte wordt ingegaan op de juridische inkadering met betrekking tot kinderporno, auteursrechten en het thema inzake de verkoop van gestolen goederen.

[7] Zie over deze waardeketenbenadering onder meer Dommering & Van Eijk (2010) en Rand Europe (2008).

1.3.1 Internetveiligheid

Artikel 4 van de richtlijn Privacy en elektronische communicatie, die in 2002 werd vastgesteld,[8] verplicht aanbieders van openbare telecommunicatiediensten (dus ook internetserviceproviders) om passende technische en organisatorische maatregelen te treffen om de veiligheid van de aangeboden diensten te garanderen. Indien nodig dient dit te gebeuren in overleg met de aanbieder van het openbare communicatienetwerk waarover de dienst wordt aangeboden. De te nemen maatregelen waarborgen een beveiligingsniveau dat in verhouding staat tot de stand van de techniek en de kosten van uitvoering ervan. Het tweede lid van het artikel bepaalt verder dat de aanbieders hun abonnees op de hoogte stellen van bijzondere risico's inzake inbreuken op de veiligheid van het netwerk. Noopt het risico tot andere maatregelen dan waartoe de dienstenaanbieder verplicht is, dan informeert hij de gebruikers over eventuele middelen om dat risico tegen te gaan met inbegrip van een indicatie van de verwachte kosten.

Recentelijk is artikel 4 uitgebreid in het kader van de herziening van het Europese kader voor de communicatiesector.[9] Lidstaten dienen de aanpassingen uiterlijk op 25 mei 2011 te implementeren. Aan het artikel wordt een nieuw lid 1bis toegevoegd. Dit legt aan aanbieders de verplichting op om de toegang tot persoonsgegevens te waarborgen, opgeslagen of verzonden persoonsgegevens te beschermen en een veiligheidsbeleid in te voeren met betrekking tot de verwerking van persoonsgegevens. De nationale toezichthouders kunnen de genomen maatregelen controleren en aanbevelingen formuleren. Een nieuw derde en vierde lid introduceren een meldplicht met betrekking tot inbreuken in verband met persoonsgegevens.[10] Inbreuken moeten worden gemeld bij de bevoegde nationale instantie. Gaat het om inbreuken in verband met persoonsgegevens die waarschijnlijk ongunstige gevolgen hebben voor de persoonsgegevens of de persoonlijke levenssfeer van een abonnee of individueel persoon, dan dient deze daarover in kennis te worden gesteld. Op nationaal niveau kunnen nadere regels worden gesteld. Ook kan de Europese Commissie technische uitvoeringsmaatregelen vaststellen.

Het oorspronkelijke artikel 4 van de richtlijn is in de Telecommunicatiewet (Tw) geïmplementeerd in artikel 11.3. Dit is inhoudelijk gelijk aan artikel 4. Recentelijk is een voorontwerp van wet tot aanpassing van de Telecommunicatiewet verschenen ter implementatie van het nieuwe richtlijnenkader.[11] Wijziging van artikel 11.3 Tw voorziet in de aanvullende bescherming met betrekking tot het beheer van persoonsgegevens en een nadere reguleringsbevoegdheid dienaangaande. In een nieuw 11.3b Tw wordt de meldingsplicht inzake inbreuken op persoonsgegevens geregeld, terwijl een hoofdstuk 11a wordt ingevoegd dat ingaat op continuïteitsvraagstukken bij openbare elektronische

[8] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 7 maart 2002 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn privacy en elektronische communicatie), PB L 201/37 (31/07/2002).
[9] Richtlijn 2009/136/EG d.d. 25/11/2009 (Burgerrechtenrichtlijn) , PB L 337/1 (18/12/2009).
[10] Zie over de meldplicht onder meer Boer & Grimmius (2009)
[11] http://www.internetconsultatie.nl/nrfimplementatie

communicatienetwerken en openbare elektronische communicatiediensten, inclusief een meldplicht met betrekking tot veiligheidsinbreuken en integriteitsverlies.

1.3.2 E-commerce richtlijn

De E-commerce richtlijn ("richtlijn inzake elektronische handel")[12] uit 2000 speelt een belangrijke rol voor internetserviceproviders. Het omvat een stelsel waarbinnen onderscheid wordt gemaakt tussen een drietal activiteiten, namelijk 'mere conduit', 'cashing' en 'hosting'.[13] Bij mere conduit (artikel 12) gaat het om het onverkort doorgeven/toegang verschaffen tot informatie. Mere conduit omvat derhalve de kernactiviteit van internetserviceproviders, namelijk het toegang verschaffen tot het internet. Wanneer zij daarbij niet verder selecteren/wijzigen sluit de richtlijn aansprakelijkheid uit. Niettemin kan de rechter of een administratieve autoriteit eisen dat een dienstenaanbieder een inbreuk beëindigt of voorkomt. Caching (artikel 13) omvat de tijdelijke, maar ongewijzigde opslag van informatie. Hosting (artikel 14) ziet op activiteiten die bestaan uit het doorgeven van informatie afkomstig van een dienstenaanbieder. Hieronder valt dus het hosten van een website of persoonlijke pagina's. Ten aanzien van caching en hosting geldt dat de richtlijn de aansprakelijkheid beperkt wanneer aanbieders informatie verwijderen nadat zij er van hebben kennis genomen (waarbij het gaat om informatie die – onmiskenbaar - onrechtmatig/onwettig is c.q. op een daartoe strekkend bevel). Dit wordt ook wel 'notice and take down' genoemd. In Nederland zijn de bepalingen van de richtlijn geïmplementeerd in artikel 6:196c Burgerlijk Wetboek. In het Wetboek van strafrecht worden bovendien tussenpersonen die medewerking verlenen bij het ontoegankelijk maken van gegevens gevrijwaard van strafrechtelijke vervolging (artikel 54a Sr).[14] Er wordt gewerkt aan een wetsvoorstel om notice and take down in strafrechtelijke zin onder te brengen in artikel 54a Sr. Verder is het de bedoeling om het wetboek van strafvordering uit te breiden met een bepaling op grond waarvan de officier van justitie medewerking kan vorderen bij het ontoegankelijk maken van strafbare inhoud op het internet.[15]

De richtlijn zegt met de bepalingen over mere conduit, caching en hosting niets over een zorgverplichting. Echter, partijen die handelen in overeenstemming met de richtlijn kunnen een beroep doen op de verminderde aansprakelijkheid. Lidstaten kunnen er evenwel voor kiezen om het notice and take down beginsel bindend voor te schrijven, de richtlijn verzet zich hier niet tegen. En marktpartijen kunnen notice and take down

[12] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel'), PbEG 2000 L 178/1

[13] Dit stelsel is weer in belangrijke mate ontleend aan de Amerikaanse Digital Millennium Copyright Act (DMCA). Hierover onder meer Elken-Koren (2006).

[14] Zie in kritische zin over artikel 54a: Schellekens, Koops, Teepe (2007).

[15] Toespraak minister Hirsch Ballin bij opstarten platform internetveiligheid d.d. 8 december 2009 (http://www.ecp-epn.nl/sites/default/files/Toespraak_mvj_8december2009.pdf)

onderdeel maken van zelfregulering. In beide situaties is sprake van een zorgplicht die valt binnen de reikwijdte van dit onderzoek.

De E-commerce richtlijn is in 2007 uitgebreid geëvalueerd in een studie van G. Spindler & T. Verbiest.[16] Deze in opdracht van de Europese Commissie verrichte studie signaleert diverse trends, die ook in dit onderzoek aan de orde komen. De invalshoek van het rapport is evenwel een andere en focust op de aansprakelijkheid van intermediairs in algemene zin.[17] De studie zou de opmaat moeten zijn naar een herziening van de E-commerce richtlijn, maar tot op heden zijn er nog geen voorstellen gedaan door de Europese Commissie. Wel zijn deze inmiddels aangekondigd in het kader van de Europese 'Digitale Agenda'.[18]

1.3.3 Identiteitsfraude

Bij identiteitsfraude op het internet gaat het om het zich toe-eigenen van de identiteit van een ander met de intentie om wederrechtelijke gedragen te begaan.[19] Definities kunnen verschillen, maar komen in de kern hierop neer. In een mededeling uit 2007 constateert de Europese Commissie dat identiteitsfraude op zichzelf niet in alle lidstaten strafbaar is gesteld.[20] Het is vaak gemakkelijker om het misdrijf als gevolg van identiteitsdiefstal te bewijzen dan de identiteitsdiefstal centraal te stellen, zo wordt gesteld. Een en ander neemt niet weg dat identiteitsfraude in strijd is met bijvoorbeeld privacy regulering. Momenteel loopt nog een onderzoek in opdracht van de Europese Commissie naar identiteitsfraude in de EU lidstaten. Mogelijk zal dit in 2012 leiden tot nadere regelgeving.[21]

1.3.4 Kinderporno

De bestrijding van kinderporno op het internet wordt in belangrijke mate gedragen door het particuliere INHOPE-initiatief, dat al in 1995 werd opgestart en door de Europese Unie ondersteund wordt.[22] INHOPE vormt de basis voor nationale meldpunten waar kinderporno kan worden gemeld (en gerelateerde activiteiten, zoals 'grooming', het online contact zoeken met kinderen met de bedoeling hen online en/of offline seksueel te misbruiken). Na verificatie van de melding wordt die doorgegeven aan de bevoegde

[16] Spindler/Verbiest 2007.
[17] Het leerstuk van aansprakelijkheid van intermediairs is volop in ontwikkeling.
[18] http://ec.europa.eu/information_society/digital-agenda/index_en.htm.
[19] Zie over identiteitsfraude onder meer: De Vries e.a. (2007); Van der Meulen (2009).
[20] Europese Commissie, mededeling van de Commissie aan het Europese parlement, de Raad en het Europees comité van de regio's naar een algemeen beleid voor de bestrijding van cybercriminaliteit, COM(2007) 267 definitief, d.d. 22 mei 2007.
[21] European Commission plan to deliver justice, freedom and security to citizens (2010-2014), Memo/10/139 d.d. 20 april 2010.
[22] International Association of Internet Hotlines, www.inhope.org

autoriteiten. In Nederland is het Meldpunt Kinderporno de partner van INHOPE.[23] De INHOPE praktijk kan worden gezien als een vorm van notice and take down.

Kinderporno staat al langer op de Europese agenda. Zo is er het Kaderbesluit van 22 december 2003, waarin wordt voorgeschreven dat lidstaten maatregelen nemen tegen onder meer de verspreiding ervan.[24] Recent is een voorstel gepubliceerd om het Kaderbesluit te vervangen door een richtlijn.[25] In artikel 21 van het ontwerp wordt voorgesteld dat lidstaten maatregelen nemen om de toegang tot kinderporno te blokkeren. Het blokkeren zou wel met de nodige waarborgen omkleed moeten zijn. Lidstaten dienen ook de nodige maatregelen te nemen om kinderporno van het internet te verwijderen. In de preambule wordt gewag gemaakt van het feit dat blokkering van belang is wanneer de informatie afkomstig is van landen die buiten de Europese rechtsmacht vallen.

Op het gebied van kindermisbruik wordt door politieautoriteiten in Europa al intensief samengewerkt in het CIRCAMP[26]-programma en is verdere samenwerking tussen Europa en de Verenigde Staten (waar de meeste kinderporno wordt gehost) aangekondigd.[27] De vorm waarin tot blokkering wordt overgaan wordt overgelaten aan de lidstaten. Zelfregulering door internetserviceproviders op basis van gedragscodes wordt als mogelijke optie genoemd (naast de mogelijkheden tot blokkering door de rechterlijke macht of politie op grond van daartoe strekkende mogelijkheden binnen het civiele en/of strafrecht). De keuze voor alternatieven is mede ingegeven door wat nationale regulering toelaat.

1.3.5 Auteursrecht

Het regime van de E-commerce richtlijn is mede ingesteld om de positie te bepalen van partijen als internetserviceproviders. Zie de eerdere paragraaf 1.4.2 voor een nadere beschrijving van de regels uit de E-commerce richtlijn. In aanvulling hierop kan worden gewezen op de discussie in het kader van het Nieuw Regelgevend Kader (NRK)[28] voor de communicatiesector over de 'three strikes'- of 'graduate response'-problematiek.[29] Voorstellen om internetserviceproviders een specifieke rol toe te kennen bij het handhaven van het auteursrecht (waarbij het in het bijzonder gaat om het downloaden van muziek,

[23] http://www.meldpunt-kinderporno.nl

[24] Kaderbesluit 2004/68/JBZ van de Raad van 22 december 2004 ter bestrijding van seksuele uitbuiting van kinderen en kinderpornografie, Pub L 13/44 d.d. 20/1/2004.

[25] Europese Commissie, Proposal for Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, Brussel, 29/3/2010, COM(2010)94 final.; zie ook: Europese Commissie, persbericht IP/10/379 d.d. 29/3/2010 en MEMO/10/107, d.d. 29/3/2010

[26] Cospol Internet Related Child Abusive Material Project (www.circamp.eu)

[27] Zie over de samenwerking Europa/VS o.a. http://www.independent.co.uk/news/media/us-eu-to-launch-programme-against-internet-child-pornography-1941748.html

[28] Het Nieuw Regelgevend Kader betreft de aanpassing van de bestaande richtlijnen voor de communicatiesector en is terug te vinden in twee richtlijnen: Richtlijn 2009/136/EG d.d. 25 november 2009, PB L 337/11 (18/12/2009) en Richtlijn 2009/140/EG d.d. 25 november 2009, PB L 337/37 (18/12/2009)

[29] Zie hierover onder meer: TNO/SEO/IVIR(2009) en Ringnalda, Elferink & De Cock Buning (2009)

video, e-boeken en games[30]) hebben uiteindelijk niet tot Europese regelgeving geleid. Wel is in artikel 3bis van de Kaderrichtlijn[31] aangeven dat bij het treffen van maatregelen door lidstaten betreffende de toegang tot of het gebruik van diensten en toepassingen door eindgebruikers, fundamentele rechten en vrijheden in acht moeten worden genomen. Nederland onderschrijft dit belang.[32]

1.3.6 Verkoop gestolen goederen

De verkoop van gestolen goederen op het internet, en meer in het bijzonder de rol daarbij van internetserviceproviders, krijgt tot op heden relatief weinig aandacht op Europees niveau. Platformaanbieders, zoals veilingsites, claimen in voorkomende gevallen dat zij hosting-diensten verrichten zoals omschreven in de E-commerce richtlijn. Hierover zijn inmiddels prejudiciële vragen aan het Hof van Justitie van de EU gesteld. Het betreft de Ebay vs L'Oreal-zaak,[33] waarin het overigens niet gaat om gestolen goederen, maar om de verkoop van op intellectuele eigendomsrechten inbreukmakende artikelen.

1.4 Onderzoeksopzet

Aan de hand van literatuurstudie is onderzoek gedaan naar de juridische en beleidsmatige context van de vijf thema's en de betrokkenheid van internetserviceproviders daarbij. De regelgeving c.q. zelfregulering is geïnventariseerd en samengevat in landenstudies.

Omdat de onderzoeksproblematiek een hoog dynamisch karakter heeft en nog volop in ontwikkeling is, is niet volstaan met traditioneel literatuuronderzoek, maar is er tevens naar gestreefd om de uitkomsten van het literatuuronderzoek te valideren en te verrijken met lokale informatie. Daartoe zijn bezoeken gebracht aan de geselecteerde landen en zijn in ieder land interviews gehouden met 6-8 betrokken partijen. Gesproken is met vertegenwoordigers van (belangenorganisaties van) internetserviceproviders, overheden, toezichthouders/handhavers, maatschappelijke organisaties en onafhankelijke deskundigen. In aanvulling hierop is in Nederland nog gesproken met verschillende organisaties/bedrijven die naast internetserviceproviders onderdeel uitmaken van de waardeketen, zoals Marktplaats/Ebay en Google. De lijst met geïnterviewde partijen is opgenomen in de bijlagen.

---

[30] Het downloaden is in sommige landen, zoals Nederland niet verboden of strafbaar, in andere landen wel. Zie literatuur vorige noot.

[31] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten (Kaderrichtlijn), PB L 108/33 (24/04/2002), gewijzigd door Richtlijn 2009/140/EG d.d. 25 november 2009, PB L 227/37 (18/12/2009).

[32] *Kamerstukken II* 2009-2010, 29838, nr. 24.

[33] http://www.judiciary.gov.uk/docs/judgments_guidance/l'oreal-ebay.pdf. Prejudiciële vragen: Publ C 267/40 d.d. 7/11/2009, zaak C-324/09)

In overeenstemming met hetgeen aan de geïnterviewden is toegezegd, zijn de uitkomsten van de gesprekken geanonimiseerd verwerkt. De onderzoekers zijn verantwoordelijk voor de interpretatie van de interviews en de wijze van verwerking.

Het literatuuronderzoek is afgesloten in april 2010. Ontwikkelingen van latere datum zijn in beperkte mate meegenomen. Het merendeel van de interviews is gehouden in de periode januari-februari 2010.

Een begeleidingscommissie onder voorzitterschap van prof. mr. F.W. Grosheide heeft de onderzoekers bijgestaan (zie bijlage). Met de commissie is de opzet van het onderzoek doorgenomen, gevolgd door een tussenrapportage. Tenslotte is het concept-rapport met de commissie besproken en zijn de opmerkingen van de commissie door de onderzoekers in het definitieve rapport verwerkt.

1.5 Indeling rapport

Hoofdstuk 1 van deze studie omvat de analyse van de onderzoeksprobleemstelling en de onderzoeksopzet. In hoofdstuk 2 ('Inventarisatie van bevindingen') wordt de (co/zelf)regulering in de onderzochte landen per thema beschreven aan de hand van de uitgevoerde landenstudies en de gehouden interviews. Hoofdstuk 3 bevat de analyse en conclusies. De landenstudies zijn als bijlage opgenomen. Zij beschrijven meer in detail de juridische inkadering en rechtsontwikkeling. Telkens wordt in een algemene inleiding eerst de implementatie van de E-commerce richtlijn geschetst, omdat die voor de meeste thema's relevant is. Per thema wordt vervolgens de bestaande bijzondere regulering geschetst (wettelijke bepalingen en overige maatregelen zoals zelfregulering) en wordt ingegaan op de toepassing van deze regulering. Waar er nog andere ontwikkelingen zijn – zoals nieuwe wetsvoorstellen – wordt dat afzonderlijk vermeld.

2 Inventarisatie van bevindingen

2.1 Inleiding

In het onderzoek is de regelgeving van de geselecteerde landen – Nederland, Frankrijk, Duitsland en het Verenigd Koninkrijk – geïnventariseerd. De relevante wet- en nadere regelgeving is in kaart gebracht. Wanneer specifieke regelgeving ontbrak is nagegaan of er mogelijk vormen van zelf/co-regulering zijn. De afzonderlijke landenstudies zijn te vinden in de bijlagen. In deze landenstudies zijn tevens verwijzingen terug te vinden naar relevante parlementaire stukken, literatuur en jurisprudentie.

Naast het inventariserend onderzoek, zijn in de vier landen meerdere interviews gehouden met betrokken partijen.

In dit hoofdstuk wordt per thema een overzicht gegeven van de stand van zaken aan de hand van de regelgeving en informatie die is verstrekt tijdens de interviews.

2.2 Internetveiligheid

In alle onderzochte landen is artikel 4 van de richtlijn Privacy en elektronische communicatie inhoudelijk terug te vinden in de nationale telecommunicatiewetten. Telkens wordt daarbij verwezen naar het belang van bescherming van de communicatieprivacy en persoonsgegevens bij elektronische communicatie. Internetveiligheid is met name in dit kader onderzocht.

Er is in de onderzochte landen verder weinig concrete invulling te vinden van de zorgplichten in dit kader. Wel is duidelijk dat internetserviceproviders worden aangesproken op in hoofdzaak twee zorgplichten. De eerste ziet op het nemen van passende technische en organisatorische maatregelen om internetveiligheid te waarborgen. De tweede ziet op het informeren van eindgebruikers over specifieke risico's, en maatregelen die tegen deze risico's genomen kunnen worden, voor zover de internetserviceprovider niet zelf gehouden is om maatregelen te nemen. Het ontbreekt in de meeste landen aan formulering van minimumvereisten of 'best practices' in nadere regelgeving dan wel jurisprudentie.

In Nederland is op initiatief van de OPTA een traject gestart om invulling te geven aan de zorgplichten die zijn neergelegd in artikel 11.3 van de Telecommunicatiewet. Dit heeft geresulteerd in een inventarisatie voor beleidsregels. Op dit moment gelden alleen regels

voor de plicht om eindgebruikers te informeren over bepaalde risico's. Deze beleidsregels zijn neergelegd in de 'Beleidsregels informatieplicht voor aanbieders over internetveiligheid'. Nadere consultatie met de Nederlandse overheid over regels met betrekking tot te nemen veiligheidsmaatregelen door internetserviceproviders staat in de planning.

De OPTA werkt samen met de KLPD op basis van een protocol waarin met name afspraken staan over informatie-uitwisseling. De KLPD kan veiligheidsinbreuken aanpakken voor zover het nationale strafrecht sancties in verband hiermee mogelijk maakt. De OPTA heeft daarnaast een eigen bevoegdheid om administratieve sancties op te leggen. Uit onderzoek blijkt dat Nederland een voortrekker is in Europa met betrekking tot diverse aspecten van internetveiligheid.[34]

Een aantal grote Nederlandse internetserviceproviders heeft een convenant gesloten waarin intenties zijn vastgelegd om gezamenlijk de bestrijding van botnets aan te pakken. Hierbij speelt informatie-uitwisseling op basis van het convenant een grote rol. Eindgebruikers zouden geholpen moeten worden om hun computers op te schonen alvorens ze weer toegang krijgen tot het internet.

In het Verenigd Koninkrijk heeft de vereniging van internetserviceproviders (ISPA UK) 'best current practices' geformuleerd, specifiek voor de veilige afhandeling van e-mail. Dit document is echter niet verplicht voor de leden.

In Duitsland kent men een nadere bepaling in de nationale telecommunicatiewet wat betreft de vereiste organisatorische maatregelen van internetserviceproviders, waarbij preventie van storingen, effecten van aanvallen van buitenaf en catastrofes als aandachtspunten worden genoemd. Verdere invulling hiervan is opnieuw overgelaten aan de betrokken partijen. Daarnaast wordt een anti-botnet website ontwikkeld op initiatief van belangenbehartiger ECO (Verband der deutschen Internetwirtschaft) en de federale overheid, waarbij in een actieve rol voor internetserviceproviders wordt voorzien bij de aanpak van gemelde of gedetecteerde botnets. Het betreft een call center dat actief meehelpt bij het opschonen van computers van klanten die zich melden. De kosten worden mede gedragen door de overheid.

In Frankrijk heeft met name spam als issue geleid tot nadere invulling vanuit de overheid. De hulplijn 'Signal Spam' is met behulp van publieke autoriteiten samen met professionele partijen opgezet. Dit initiatief kan in het verlengde worden gezien van aanbevelingen die de Franse belangenvereniging van internetserviceproviders (AFA) heeft opgesteld over technische maatregelen tegen spam.

[34] Dumortier & Somers (2008).

De Franse regering heeft onlangs voorstellen gedaan voor een wettelijke regeling als gevolg waarvan onder andere internetserviceproviders bepaalde veiligheidsinbreuken in relatie tot persoonsgegevens moeten melden aan de Franse toezichthoudende autoriteit op dit gebied (CNIL). Dit voorstel kan gezien worden als een vroege invulling van het recentelijk uitgebreide artikel 4 van de richtlijn Privacy en elektronische communicatie. In zowel Nederland als Frankrijk heeft de overheid de intentie uitgesproken ook andere diensten van de informatiemaatschappij, dus niet alleen internetserviceproviders, daartoe te verplichten.

In de interviews is benadrukt dat er nadere invulling nodig is van de zorgplichten die voortvloeien uit het (nieuwe) Europese richtlijnenkader. De geïnterviewde partijen hebben in het algemeen aangegeven dat controle van internetverkeer in verband met veiligheid stuit op privacy wetgeving, met name op wetgeving met betrekking tot het (tele)communicatiegeheim. Technisch zijn er wel mogelijkheden. Op basis van hun overeenkomsten met klanten filteren internetserviceproviders in verband met virussen en spam. Verschillende partijen hebben zorgen geuit over onduidelijkheid van het wettelijke kader over de toelaatbaarheid van dergelijke methodes. Er bestaat weinig transparantie over wie door deze methodes worden geraakt, en in welke mate.

Botnets zijn een duidelijke zorg voor internetserviceproviders. In de interviews is dit probleem besproken als apart aandachtspunt binnen het thema internetveiligheid en het wettelijk kader voortkomend uit de implementatie van artikel 4 van de richtlijn Privacy en elektronische communicatie. Internetserviceproviders kunnen te maken krijgen met notering op blacklists als gevolg van botnets, waardoor bepaalde diensten, zoals e-mail, kunnen worden ontwricht. Hoewel er veel publieke bronnen met locatiegegevens over botnets beschikbaar zijn, is het moeilijk om ze allemaal te vangen en is de afhandeling daarvan arbeidsintensief. Ook is het achterhalen van de betrouwbaarheid van de genoemde publieke bronnen een lastige fase.[35] Quarantaine maatregelen voor dergelijke computers lijken noodzakelijk, maar hebben als negatief aspect dat ze straffend van karakter zijn. Verschillen in beschikbare middelen betekenen daarnaast dat niet alle internetserviceproviders zullen (willen) optreden tegen botnets bij hun klanten.

Risico's bij het gebruik van draadloze routers hebben speciale aandacht gekregen. Er is in de interviews de vraag gesteld of de bestaande zorgplichten op gebied van internetveiligheid dit thema tevens omvatten. Duidelijk is dat er naast internetserviceproviders, verschillende andere marktpartijen zijn die draadloze routers leveren. Het huidige telecommunicatie-rechtelijke kader heeft ten aanzien van deze partijen geen reikwijdte.

In de interviews is eveneens de vraag gesteld in hoeverre bij de informatieplicht voor internetserviceproviders in verband met artikel 4 richtlijn Privacy en elektronische communicatie, wordt toegezien op de effectiviteit van de genomen maatregelen. De vraag is aan de orde geweest of de nationale overheid een actieve rol zou kunnen spelen bij het

instrueren van eindgebruikers over de veiligheid en beveiliging van het internet, en meer zou kunnen toezien of de informatie eindgebruikers ook daadwerkelijk bereikt.

In verband met internetveiligheid is de vraag gesteld welke publieke autoriteiten betrokken kunnen zijn bij veiligheidsinbreuken. In het algemeen geldt dat dit afhankelijk is van de mate waarin een veiligheidsinbreuk een kwestie is van nationale veiligheid. Met name in Frankrijk heeft dit gevolgen voor competenties, aangezien de nationale telecommunicatie autoriteit aldaar (ARCEP) niet de status heeft om kwesties van nationaal veiligheidsbeleid aan te pakken. Andere autoriteiten op het gebied van privacy en nationale defensie zouden een rol kunnen spelen, maar deze is nog niet nader gedefinieerd of er is weinig over bekend.

2.3 Kinderporno

Al vóór de E-commerce richtlijn was er ruime aandacht voor het thema kinderporno. In de praktijk is er sprake van nadruk op notice and take down via een systeem van meldpunten in het kader van INHOPE, de Europese organisatie op dit gebied. De websites van deze meldpunten fungeren als de eerste ingang voor meldingen. In het algemeen is de aandacht enkel gericht op het publiekelijk toegankelijke internetverkeer, met name websites. Deze meldpunten spelen een actieve rol in het afhandelen van meldingen over kinderpornografie, waarbij actief wordt samengewerkt met politie en justitie, ook internationaal. Internetserviceproviders sturen meldingen veelal direct door naar deze meldpunten.

In sommige landen zijn daarnaast gedragscodes ontwikkeld die mede zien op aanbevelingen voor notice and take down in relatie tot kinderporno.

Binnen het kader van de 'European Framework for Safer Mobile Use' hebben aanbieders van mobiele telefonie in alle onderzochte landen raamwerk-afspraken ondertekend, waarbinnen ook aandacht wordt besteed aan toegang tot kinderpornografisch materiaal. De aanbieders verklaren hierin voor zichzelf een zorgplicht te zien om bij te dragen aan de verwijdering van kinderpornografie op internet.

In Nederland is een 'Gedragscode Notice and takedown' ontwikkeld door het NICC. De code wordt nu onderhouden in het kader van het Platform Internetveiligheid. In dit platform werken overheid en marktpartijen samen. De gedragscode is een intentieverklaring waarbij onder meer de grootste internetserviceproviders zijn aangesloten. Dienstenaanbieders in het algemeen kunnen de code gebruiken voor de ontwikkeling van notice and take down procedures. De gedragscode beoogt een brede

[35] Zie in dit verband onder meer: Van Eeten e.a. (2010).

reikwijdte te bieden wat betreft toepassing van notice and take down procedures op illegale en onrechtmatige content op het internet. De afhandeling van dergelijke procedures wordt in hoofdzaak bij de aanbieders zelf gelegd. Er wordt verder geen rol van de rechterlijke autoriteiten beschreven. De wettelijke basis voor een notice en take down bevel door een officier van justitie in een strafrechtelijke context in het Wetboek van Strafrecht behoeft verduidelijking, met name voor wat betreft de waarborgen voor een afdoende rechterlijke toetsing van een dergelijk bevel. De ontwikkeling hiervan is bij de implementatie van de E-commerce richtlijn aangekondigd maar is tot op heden nog niet voltooid. Zowel in de literatuur als in recente rechtspraak is het ontbreken van dergelijke waarborgen gesignaleerd.

Er zijn in Nederland verschillende partijen die plannen voor het filteren van internetverkeer op kinderporno ondersteunen, zoals het Meldpunt Kinderporno en het Platform Internetveiligheid. In het kader van het laatste platform, met betrokkenheid van de Nederlandse overheid, is de ontwikkeling aangekondigd van een zwarte lijst, te gebruiken voor filtering door internetserviceproviders.

In het Verenigd Koninkrijk valt de Internet Watch Foundation (IWF) op, die als non-gouvernementele organisatie de rol van meldpunt vervult in verband met kinderporno. De IWF vervult op basis van zelfregulering een verbindende rol die niet alleen internetserviceproviders en experts bij elkaar brengt, maar ook educatieve instellingen en het algemene publiek bij de bestrijding van kinderporno betrekt. De IWF neemt niet alleen de evaluatie van meldingen over kinderporno op zich, met doorverwijzing naar (internationale) opsporingsautoriteiten, maar genereert ook een blacklist die door een groot percentage van internserviceproviders in het Verenigd Koninkrijk wordt gebruikt voor blokkering van kinderporno op internet. De belangenvereniging van internetserviceproviders (ISPA UK) verwijst in haar gedragscode ook naar de rol van de IWF.

De Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) is een zelfreguleringsorgaan in Duitsland. De FSM heeft, naast een meldpunt, ook een gedragscode voor haar leden, waaronder alle grote internetserviceproviders zijn te vinden. De code vereist een actieve rol van de leden bij de bestrijding van kinderporno, waaronder een plicht tot het doorsturen van meldingen aan opsporingsinstanties, en biedt mogelijkheden om de leden te waarschuwen dan wel uit de organisatie te zetten indien ze niet aan de code voldoen.

Een recent aangenomen wet in Duitsland (Zugangserschwerungsgesetz) die voorziet in een rol voor internetserviceproviders om op basis van een lijst, op te stellen door de landelijke politiedienst (Bundeskriminalamt), kinderpornografisch materiaal te blokkeren, lijkt te worden afgeschaft. In verband hiermee had de Duitse overheid ook individuele contracten opgesteld met internetserviceproviders, waarvan de inhoud verder niet bekend is. Er is veel weerstand getoond tegen de wet en deze contracten vanwege de ingrijpende inbreuk op het

communicatiegeheim, en op de privacy en vrijheid van meningsuiting in het algemeen. Er zijn geen initiatieven genomen om de beoogde lijst daadwerkelijk samen te stellen en er wordt gekeken hoe de wet kan worden teruggedraaid. Dit is ook bevestigd in de interviews.

Frankrijk kent een wettelijk ingekaderde notice and take signaleringsprocedure voor bepaalde, nader vastgestelde categorieën 'bijzonder schadelijke illegale content', waaronder kinderpornografie. Internetserviceproviders hebben als gevolg hiervan een wettelijke plicht om meldingen van kinderpornografie door te spelen aan alle betrokken publieke autoriteiten.

Daarnaast is in Frankrijk een gedragscode ontwikkeld door de belangenvereniging van internetserviceproviders (AFA), die inhoudelijk lijkt op de 'Gedragscode Notice and take down' in Nederland. Wel ziet de Franse code alleen op bepaalde categorieën illegale content, waaronder kinderpornografie.

In Frankrijk heeft het discussieplatform 'Forum des droits sur l'Internet' diverse aanbevelingen in relatie tot kinderpornografie op het internet gedaan. Een daarvan heeft geleid tot plannen op regeringsniveau om verplichtingen tot filtermaatregelen in verband met kinderporno voor internetserviceproviders te ontwikkelen.

In de interviews is naar voren gekomen dat internetserviceproviders in verband met kinderporno bereid zijn om mee te werken aan de bestrijding ervan, maar dat zij wel op hun hoede zijn voor te ver gaande maatregelen in verband met hun eigen aansprakelijkheid, in het licht van de beperkingen van aansprakelijkheid in de E-commerce richtlijn. Ook is gewezen op het gevaar voor een hellend vlak naar andere gebieden dan kinderporno.

Men is over het algemeen tevreden over de werking van het INHOPE meldpuntensysteem. Als voordeel wordt onder andere genoemd de mogelijkheid van delegatie naar de meldpunten van het vereiste om materiaal dat gemeld wordt, te classificeren. Teveel betrokkenheid bij classificering zou internetserviceproviders aanzetten tot blindelings ingrijpen. Dit zou tot een onnodig sterk gecensureerd internet kunnen leiden. Ditzelfde zou kunnen gebeuren als er meer praktijken zouden ontstaan naast de meldpunten, met name als gewerkt zou worden met zogenaamde 'blacklists'.

Op basis van de interviews lijkt actieve controle van internetverkeer, waarbij bijvoorbeeld deep packet inspection wordt gebruikt, niet te worden toegepast. Deep packet inspection wordt als een niet-proportionele maatregel beschouwd, zo is de stelling van een zeer grote meerderheid van de geïnterviewden.

Verschillende partijen hebben (grote) twijfels geuit over de effectiviteit van filtermaatregelen. Zij waarschuwden ook voor de ontwikkeling van nieuwe encryptie

technieken en moeilijk te detecteren netwerken van verspreiding, als negatief effect van actieve filtering door internetserviceproviders.

Uit de interviews blijkt dat er verschillende beleidsdoelen worden aangedragen als motivatie voor plannen tot filterverplichtingen in relatie tot kinderporno. Naast bestrijding van kinderpornografie, met bescherming van kinderen als hoofddoel, is het voorkomen van ongewenste confrontatie genoemd.

In de interviews is naar voren gekomen dat de politie soms over te weinig middelen en deskundig personeel beschikt. Traditionele opsporingsmethoden voor de bestrijding van kinderporno staan veelal centraal bij de opsporingsinstanties.

Diverse geïnterviewde partijen benadrukten het belang van goede begeleiding van ouders bij de opvoeding van kinderen omtrent verstandig gebruik van het internet.

Verschillende partijen hebben verwezen naar de praktijk in de Verenigde Staten waarbij marktpartijen uit de financiële sector samenwerken om transacties te controleren ter bestrijding van toegang tot kinderporno op internet.

2.4 Auteursrecht

Net als bij het thema kinderporno, is de regelgeving die is geharmoniseerd door de E-commerce richtlijn in alle onderzochte landen het bepalende juridische kader voor het thema auteursrecht. De zorgplicht van internetserviceproviders ziet op basis hiervan alleen op maatregelen tot verwijdering achteraf in de vorm van notice and take down procedures, in de context van 'caching' en 'hosting' activiteiten.

De praktijk van notice and take down is in relatie tot auteursrecht minder strak ingekaderd dan omschreven bij het thema kinderpornografie. Wel kennen het Verenigd Koninkrijk en Frankrijk wettelijke initiatieven om zogenaamde 'graduated response' systemen in het leven te roepen. In Frankrijk is de totstandkoming van de hiervoor onder de naam HADOPI[36] bekend geworden wetgeving inmiddels afgerond. In het Verenigd Koninkrijk is recent de Digital Economy Act aangenomen.

In Nederland kent men als gevolg van jurisprudentie over de aansprakelijkheid van bepaalde internet(diensten)aanbieders, een nadere discussie over de grenzen aan de zorgplicht van internetserviceproviders. Deze rechtszaken (zie de landenstudie) hebben zich met name bij rechters in lagere instanties afgepeeld. Veelal draaide het om websites die

[36] De wet heet officieel *Loi favorisant la diffusion et la protection de la création sur Internet*, maar wordt meestal als 'Loi HADOPI' aangeduid, naar de naam van de nieuwe toezichthouder die in de wet is opgenomen, de *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*

geen aanspraak konden maken op de status van 'hosting' en op de bijbehorende beperking van aansprakelijkheid zoals geïmplementeerd uit de E-commerce richtlijn. Er was telkens sprake van dusdanige betrokkenheid bij auteursrechtinbreuken dat daardoor geen sprake is van de beperkte omschrijving van 'hosting' activiteiten in de zin van deze richtlijn. Een enkele maal is een internetserviceprovider in een voorlopige voorzieningsprocedure door de rechter bevolen in te grijpen in verband met het verlenen van toegang aan een websitehouder die op onrechtmatige wijze auteursrechtinbreuk faciliteerde. In de literatuur is er veel kritiek op deze uitspraak.

Recent heeft in Nederland op parlementair niveau de privé-exceptie in de huidige Auteurswet, op basis waarvan het kopiëren, en dus ook downloaden, van auteursrechtelijk beschermd materiaal voor privé doeleinden is vrijgesteld van auteursrechtelijke aanspraken door rechthebbenden, ter discussie gestaan. Een dergelijk exceptie is in de overige onderzochte landen niet in de auteursrechtwetgeving te vinden. Een parlementaire commissie in Nederland heeft voorgesteld om ten aanzien van het downloaden van de bestaande exceptie te schrappen. Bij deze discussie is tevens aan de orde gekomen of en op welke manier internetserviceproviders een rol kunnen spelen bij de handhaving van het voorgestelde nieuwe verbod. Er zijn voorstellen gedaan om hiervoor technieken te gebruiken waarmee het internetverkeer structureel kan worden gecontroleerd op het niveau van doorgegeven bestanden, zoals 'deep packet inspection' en 'finger printing'. Bovendien dient volgens de commissie wettelijk te worden geregeld dat Nederlandse internetserviceproviders of hostingproviders klantgegevens beschikbaar hebben van personen of bedrijven die via hun infrastructuur websites opzetten. De Nederlandse regering heeft in een eerste reactie aangegeven het met de werkgroep eens te zijn dat er op verschillende terreinen van het auteursrecht problemen bestaan die moeten worden aangepakt. De voorstellen van de commissie hebben op dit moment nog niet tot concrete wetsvoorstellen geleid. Wel heeft de commissie laten weten dat zij niet langer het gebruik van deep packet inspection als een optie ziet.[37]

In het Verenigd Koninkrijk wordt de zorgplicht van internetserviceproviders op basis van de huidige wetgeving gebaseerd op de aansprakelijkheidsbeperkingen van de E-commerce richtlijn. Recent is een nieuwe wet (Digital Economy Act) aangenomen. Op grond van deze nieuwe wet zouden internetserviceproviders meldingen van rechthebbenden actief moeten doorspelen aan vermeende inbreukmakers. De providers zouden op basis van de nieuwe bepalingen ook lijsten moeten bijhouden van eindgebruikers die onderwerp zijn geweest van dergelijke meldingen. Deze lijsten met identificerende data zouden zij beschikbaar moeten stellen aan rechthebbenden om behulpzaam te zijn bij het ontdekken van herhaalde inbreuk door eindgebruikers. Deze lijsten mogen echter niet de identiteit van de internetgebruiker openbaren. Wanneer het doorspelen van meldingen niet resulteert

[37] *Kamerstukken II*, 2009-10, 29838, nr. 28.

in de beëindiging van inbreukmakende activiteiten door inbreukmakers, zouden op basis van de nieuwe wet van internetserviceproviders technische beperkingen van het gebruik van internetverbindingen door hun klanten gevraagd kunnen worden.

In Duitsland is de implementatie van de E-commerce richtlijn bepalend voor de zorgplicht van internetserviceproviders in relatie tot auteursrecht op het internet. De Duitse regelgeving volgt de richtlijn.

In Frankrijk heeft de nieuwe wetgeving, onder de naam HADOPI, geleid tot nieuwe plichten van internetserviceproviders. Deze zijn nieuw ten opzichte van de zorgplichten die voortvloeien uit de E-commerce richtlijn in relatie tot 'mere conduit', 'caching' en 'hosting' activiteiten door internetserviceproviders.

In verband met de plicht van eindgebruikers om hun internetverbinding dusdanig in te richten dat auteursrechtinbreuk wordt voorkomen, een verplichting die is neergelegd in de Franse auteurswet, moeten internetserviceproviders voorlichting geven over maatregelen die hiervoor geschikt zijn. Deze voorlichting moet gebaseerd worden op een lijst die opgesteld wordt door de in de nieuwe wetgeving in het leven geroepen HADOPI autoriteit (Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet). Internetserviceproviders moeten daarnaast eindgebruikers in hun gebruikers-overeenkomsten informeren over de mogelijke sancties op het niet naleven van de genoemde verplichting. Indien de autoriteit samen met de rechterlijke instanties besluit om in te grijpen, kan aan internetserviceproviders worden verzocht om aan eindgebruikers waarschuwingse-mails te sturen (waarin het ongeoorloofde gebruik wordt gesignaleerd) dan wel, ingeval van voortdurende nalatigheid, om internetverbindingen af te sluiten. Indien internetserviceproviders hieraan niet zouden meewerken, bestaat de mogelijkheid van een boete.

De HADOPI wetgeving is van zeer recente datum. Nadere regelgeving is nog niet vastgesteld. De beoogde lijst met maatregelen die eindgebruikers kunnen gebruiken voor beveiliging van hun verbindingen, op basis waarvan internetserviceproviders eindgebruikers moeten adviseren, is ook nog niet opgesteld. Er zijn ook nog geen waarschuwingse-mails verzonden.

De interpretatie in de Franse jurisprudentie van de zorgplichten van internetserviceproviders heeft zich met name gericht op de beperking van aansprakelijkheid voor 'hosting' activiteiten, zoals geformuleerd in de implementatiewetgeving van de E-commerce richtlijn. Net als in Nederland, gaat het hier veelal om interpretaties door rechters in de lagere instanties. Vaak ging het om de interpretatie van het moment waarop 'hosting' providers geacht kunnen worden op de hoogte te zijn van onmiskenbaar onrechtmatig materiaal, hetgeen in de formulering van de aansprakelijkheidsbeperking vereist is om ingrijpen als verplichting van 'hosting' providers te kunnen vaststellen. Een enkele maal is een 'hosting' provider bevolen om na de eerste

verwijdering van een website op basis van haar zorgplicht, iedere herhaalde poging om dezelfde content opnieuw op het internet te plaatsen, tegen te gaan.
In de interviews is in het algemeen benadrukt dat de maatregelen die rechthebbenden graag zouden willen zien, al snel buiten de kaders van de aansprakelijkheidsbeperkingen van de E-commerce richtlijn vallen. Internetserviceproviders aan wie gevraagd wordt om inbreukmakend internetverkeer op te sporen en te blokkeren, lopen het risico zelf aansprakelijk te kunnen worden gesteld. Daarnaast zijn twijfels geuit over de technische haalbaarheid van detectie van inbreukmakend materiaal dat wordt doorgegeven of opgeslagen door internetserviceproviders. Als mogelijkheid is wel genoemd het versturen van waarschuwingse-mails na vaststelling van het inbreukmakend karakter van bepaald materiaal.

Wat betreft de HADOPI wetgeving hebben partijen in de interviews daarover veel twijfels geuit. Zij waarschuwen ervoor dat dergelijke sterke wetgeving zou kunnen leiden tot ontwikkeling en algemeen gebruik van encryptie technologie voor de verspreiding van auteursrechtelijk beschermd materiaal. Dezelfde technologie zou dan gebruikt kunnen worden voor illegale content in het algemeen. Sommigen benadrukten dat internetserviceproviders niet in de positie gebracht moeten worden dat ze internetverkeer moeten monitoren of moeten bijdragen aan punitieve maatregelen tegen eindgebruikers. Er zijn ook veel twijfels geuit over de capaciteit van internetserviceproviders en de rechterlijke instanties om de actieve aanpak van auteursrecht op basis van de HADOPI wetgeving te ondersteunen. Ook opsporingsinstanties stelden de proportionaliteitsvraag en wezen op de relatie tot andere opsporingsactiviteiten met betrekking tot cybercrime.

Sommige partijen hebben bepleit dat internet meer gezien moet worden als een universele dienst waarmee ingrijpende maatregelen door internetserviceproviders onverenigbaar zijn.
Plannen voor soortgelijke wetgeving als de Franse HADOPI regelgeving lijken in de andere landen steeds terughoudender te worden benaderd. Veel partijen hebben ook terughoudendheid bepleit om wetgeving als de HADOPI regelgeving over te nemen. Er zijn nog geen ervaringen met de effectiviteit en toepasbaarheid van dergelijke regelgeving

In het kader van de Britse Digital Economy Act zijn vergelijkbare vragen opgeworpen. Ten aanzien van zowel de Franse als Britse regelgeving is verder aan de orde hoe zij zich verhouden tot het nieuwe artikel 1, lid 3 bis van de Kaderrichtlijn. Hierin is bepaald dat maatregelen van de lidstaten betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken de fundamentele rechten en vrijheden van natuurlijke personen, zoals die door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht worden gewaarborgd, dienen te eerbiedigen. Het artikel verstaat hieronder mede privacy en regels met betrekking tot een eerlijke en transparante rechtsgang.

2.5 Identiteitsfraude

In geen van de landen is het zich toe-eigenen van iemands identiteit op zichzelf strafbaar gesteld. Dit betekent dat op basis van de beperkingen aan aansprakelijkheid voor internetverkeer, zoals geformuleerd door de E-commerce richtlijn en als zodanig geïmplementeerd in alle onderzochte landen, internetserviceproviders geen bijzondere zorgplicht hebben ten aanzien van identiteitsfraude.

Het probleem van identiteitsfraude online is met name in verband gebracht met andere dienstenaanbieders op het internet, zoals sociale netwerk websites en de banken die online transacties faciliteren. Deze partijen kunnen vanwege hun betrokkenheid bij het internetverkeer waarmee identiteitsfraude wordt gepleegd, geen aanspraak maken op de aansprakelijkheidsexcepties van de E-commercerichtlijn.[38]
In Nederland is er op parlementair niveau discussie geweest over het belang van een meldplicht omtrent veiligheidsinbreuken voor internetserviceproviders waarbij persoonsgegevens betrokken zijn. Dit zou kunnen bijdragen aan het tegengaan van identiteitsfraude op het internet. Deze meldplicht is gerelateerd aan het nieuwe artikel 4 in de richtlijn Privacy en elektronische communicatie waarin een dergelijke plicht is opgenomen voor internetserviceproviders, zoals besproken bij het thema internetveiligheid.

In het Verenigd Koninkrijk is onlangs de Fraud Act 2006 aangenomen waarin een algemene strafbaarstelling van fraude is opgenomen. Deze wet is opgesteld om ook opkomende praktijken in verband met nieuwe technologieën te kunnen omvatten.

Binnen het debat in Duitsland is met name 'phishing' als frauduleuze praktijk op het internet besproken. 'Phishing' is de praktijk waarbij door middel van het kopiëren van bestaande websites een zekere betrouwbaarheid van deze kopieën wordt gefingeerd terwijl het valse websites betreft. Deze 'phishing websites' worden gebruikt om gebruikers uit te lokken hun identificerende gegevens, zoals inloggegevens, te verstrekken. De discussie spitste zich toe op de vraag of onder de huidige strafwetgeving, dergelijke praktijken strafbaar kunnen zijn. Er worden wel bepalingen aangewezen die 'phishing' kunnen omvatten.

In Frankrijk kent men een voorstel voor het strafbaar stellen van toe-eigening van iemands identiteit. Daarnaast is een technisch hulpmiddel (IDéNum) ontwikkeld waarmee de authenticiteit van een claim online omtrent iemands identiteit zou kunnen worden vastgesteld.[39] De Franse overheid is de initiatiefnemer van dit middel en heeft het ter beschikking gesteld voor algemeen gebruik door dienstenaanbieders.

---

[38] Dit laat natuurlijk onverlet dat algemene aansprakelijkheidsregels en privacyregulering op hen van toepassing is.

[39] http://www.idenoum.com/

Uit de interviews is naar voren gekomen dat het moeilijk denkbaar is om internetserviceproviders direct te laten meewerken aan de aanpak van identiteitsfraude online. Als voorbeeld is de bestrijding van 'phishing' besproken. Effectieve bestrijding door internetserviceproviders wordt met name bemoeilijkt omdat frauduleuze websites slechts kortstondig gebruik maken van bepaalde IP-addressen of in het buitenland worden gehost. Sommige internetserviceproviders hebben aangegeven binnen deze technische grenzen wel actie te ondernemen na meldingen van 'phishing' websites, om zoveel mogelijk te voorkomen dat ze vanwege hosting van dergelijke websites op blacklists komen. Andere maatregelen zijn technisch moeilijk toepasbaar en komen in conflict met het recht op communicatiegeheim en op bescherming van de privacy. Sommige partijen waarschuwden voor het betrekken van teveel onderwerpen onder de verantwoordelijkheid van internetserviceproviders.

In het algemeen werden internetserviceproviders niet aangewezen als de in dit kader aan te spreken partijen. Sociale netwerking sites, banken en creditcardmaatschappijen zijn genoemd als relevante aanspreekpunten.[40] Overigens nemen deze partijen – al dan niet samen met de overheid - vaak al initiatieven om fraude tegen te gaan.

Verdere educatie van eindgebruikers is meerdere malen genoemd als een belangrijk element bij het tegengaan van identiteitsfraude en heeft in diverse landen geleid tot ondermeer publiekscampagnes.

2.6 Verkoop gestolen goederen

De verkoop van gestolen goederen, in Nederlandse begrippen aan te duiden als schuldheling, is met name bediscussieerd in relatie tot platforms zoals die van – het wereldwijd opererende – eBay, dat in de onderzochte landen dominant is (ook het Nederlandse Marktplaats.nl is in handen van eBay). Veiling- en verkoopplatforms blijken de belangrijkste speler te zijn bij het vraagstuk van de verkoop van gestolen goederen via het internet. Uit de interviews kan worden afgeleid dat daarbuiten zich weinig significante problematiek voordoet (althans voor zover voor dit onderzoek relevant). De conclusie is dat de E-commerce richtlijn het juridisch kader vormt waarbinnen de discussie over dit thema plaatsvindt. Het fundamentele vraagstuk daarbij is de status van deze platforms. In verband met inbreuk op intellectuele eigendomsrechten door de op veiling- en verkoopplatforms aangeboden goederen, is in rechtszaken op verschillende niveaus tot op heden een wisselend beeld ontstaan. Alle landen kennen jurisprudentie op dit gebied. Er is geen eenduidige categorisering van deze platforms in de termen van de E-commerce richtlijn.

[40] Zie onder meer: Van der Meulen (2006) en (2009); Vermissen (2009).

In Nederland is in de rechtspraak de status van veilingsites als eBay en Marktplaats in relatie tot de E-commerce richtlijn niet nader ingekaderd. In jurisprudentie zijn wel verschillende verzoeken voor maatregelen in verband met de verkoop van op intellectuele eigendomsrechten inbreukmakende goederen in het kader van het algemene aansprakelijkheidsrecht beoordeeld. Notice and take down wordt daarin bestempeld als proportionele maatregel in het licht van de vereiste zorgvuldigheid die van deze websites kan worden gevraagd. Preventieve filtering van te plaatsen advertenties of het verplicht verzamelen van naam-, adres- en woonplaatsgegevens van adverteerders worden in deze jurisprudentie niet erkend als gepaste maatregelen.

In L'Oréal v. eBay[41] heeft de High Court van het Verenigd Koninkrijk in het voordeel van eBay geoordeeld en deze organisatie vrijgesproken van aansprakelijkheid voor door gebruikers aangeboden materiaal dat inbreuk maakt op het merkrecht van anderen.

Het Bundesgerichtshof in Duitsland heeft in drie verschillende zaken uitgemaakt dat online veilingwebsites, in tegenstelling tot internetserviceproviders en andere tussenpersonen, indirect aansprakelijk zijn voor het aanbieden van namaakgoederen (*Störerhaftung*). Daarnaast heeft het hof een preventieve voorziening voor rechthebbenden tegen veilingwebsites ontwikkeld. Dit betekent dat veilingwebsites een zorgplicht hebben om in de toekomst inbreuken op intellectueel eigendomsrecht door gebruikers, die reeds als potentiële inbreukmakers zijn aangemerkt, te voorkomen. Het hof heeft bepaald dat het gebruik van filtersoftware hierbij kan helpen en dat zulke maatregelen niet disproportioneel zijn.

Verschillende rechters in Frankrijk, waaronder een hoger beroepsrechter, hebben bepaald dat eBay dient te worden aangemerkt als hosting provider en dat zij niet gehouden is preventief onderzoek te doen naar de integriteit van geplaatste advertenties. Het Gerecht van Eerste Aanleg in het Handelsrecht heeft echter in drie beslissingen in 2008 geweigerd eBay te kwalificeren als hosting provider. eBay werd door dit gerecht aansprakelijk gehouden voor het gebrek aan toezicht en het nalaten van het nemen van efficiënte en geschikte maatregelen tegen de verkoop van namaakproducten.

In Frankrijk kent men een aantal aanbevelingsdocumenten, opgesteld door expertgroepen met initiatief vanuit de regering. Een daarvan ziet op de handel in cultuurgoederen, en beveelt onder andere een register van (gestolen) cultuurgoederen aan. Een ander richt zich specifiek op samenwerking tussen online verkoopplatforms en merkhouders om de online handel in namaakgoederen tegen te gaan. Op het niveau van de overheid heeft in Frankrijk discussie plaatsgevonden over nadere aanduiding van welke activiteiten van de platformaanbieders zouden vallen onder de uit de E-commerce richtlijn overgenomen beperking van aansprakelijkheid voor 'hosters'. De aanbevelingen en discussie daarover hebben tot op heden geen verandering gebracht in de wettelijke regels.

[41] zie paragraaf 1.3.6.

In de interviews is breed onder de aandacht gebracht dat internetserviceproviders niet in alle gevallen de aangewezen partijen zijn voor regulering van de online verkoop van gestolen goederen. Sommigen van de internetserviceproviders hebben aangegeven ook nog nooit een verzoek tot ingrijpen in verband met gestolen goederen te hebben gekregen. Anderen gaven aan wel op verzoek te zullen samenwerken met justitie en politie. Controle van internetverkeer op dit aspect is niet effectief en ook technisch onuitvoerbaar. Een formele zorgplicht zou leiden tot overmatig ingrijpen door internetserviceproviders en eventueel tot een glijdende schaal naar andere gebieden. Ingrijpen in verband met illegale content in het algemeen ligt op de loer en zou leiden tot disproportionele beperkingen van economische ontwikkeling op het internet.

In het algemeen wordt gewezen naar de platformaanbieders die de verkoop van goederen online faciliteren. Zij hebben aanleiding gegeven tot zelfregulering waarbij de reacties van gebruikers van een dergelijk platform een belangrijke motivatie opleveren om voor dit probleem verantwoordelijkheid te nemen. Deze zorgplicht resulteert met name in vormen van notice and take down procedures bij de websites van eBay en op Marktplaats.nl, waarbij deze partijen verwijzen naar de aansprakelijkheidsexceptie die vanuit implementatie van de E-commerce richtlijn geldt voor dienstenaanbieders die 'hosting' activiteiten verrichten. Die zou naar hun mening ook op hen van toepassing zijn.

Platforms voor de online verkoop van goederen hebben verschillende initiatieven genomen gericht op een procedurele afhandeling van klachten over aanbiedingen van gestolen goederen en namaakgoederen. Daarnaast worden gebruikers geïnformeerd over bestaande procedures en over de regelgeving die van toepassing is.

Er is samenwerking met justitie en politie, die kunnen rekenen op een actieve respons van de platformaanbieders. Over reacties van de oorspronkelijke eigenaren van gestolen goederen wordt ook actief overlegd met justitie en politie. Wel leiden kwesties over de verkoop van gestolen goederen en oplichting vaak tot de conclusie dat het een civiele zaak betreft (bijvoorbeeld met betrekking tot het vorderen van vergoeding van geleden vermogenschade).

Rechthebbenden op intellectuele eigendom, met name merkhouders, leggen veel druk op platformaanbieders. Verschillende rechtszaken laten de door hen gevraagde maatregelen zien. Deze maatregelen worden gedeeltelijk opgevangen door de procedure via het Verified Right Owner Program (VeRO), waarin met name door eBay is geïnvesteerd,.[42] Deze procedure ziet onder meer op identificatie van rechthebbenden en op het vaststellen van connecties met advertenties op de platforms achteraf.

[42] http://pages.ebay.nl/vero/

3 Analyse en conclusies

3.1 Inleiding

Het onderwerp van het onderzoek bevindt zich in een dynamische omgeving. In aanvulling op de schets in het vorige hoofdstuk, komen hier enige algemene observaties aan de orde en worden conclusies geformuleerd.

3.2 Waardeketen

De onderzoeksvraag richt zich op zorgplichten in de relatie tussen de overheid en internetserviceproviders. Internetserviceproviders staan zowel op nationaal als internationaal niveau volop in de belangstelling, niet alleen voor wat betreft hun verhouding tot de overheid, maar ook ten opzichte van andere privaatrechtelijke partijen, bijvoorbeeld met betrekking tot de (civielrechtelijke) aansprakelijkheidproblematiek. Dit onderzoek richt zich op de eerste relatie. Waar deze ontbreekt is wel nagegaan of er mogelijk elders in de waardeketen waarvan internetserviceproviders deel uitmaken zorgplichten spelen.

In paragraaf 1.3 is al aangegeven dat internetserviceproviders behoren tot degenen die actief zijn in de (economische) waardeketen tussen eindgebruikers en de aanbieders van diensten. Wanneer we de vijf thema's tegen het licht houden wordt dit ook bevestigd. Op onderdelen zijn specifieke zorgplichten voor internetserviceproviders te onderkennen. Deze komen onder meer voort uit sectorspecifieke regulering of zijn een uitvloeisel van de regels met betrekking tot E-commerce. Bij andere thema's is duidelijk dat zorgplichten eerder in relatie worden gezien met andere partijen in de waardeketen, meer in het bijzonder met de partijen die specifieke diensten aanbieden of deze op platformniveau faciliteren.

Het leggen van verantwoordelijkheid bij internetserviceproviders lijkt op het eerste oog een eenvoudige optie. Het zijn immers de internetserviceproviders die de toegang controleren van eindgebruikers tot het internet. Internetserviceproviders zijn 'gatekeepers' en vervullen een 'bottleneck'-functie.

Tegelijkertijd wordt duidelijk dat een dergelijke benadering zich in steeds mindere mate verdraagt met de dynamiek van het internet (zoals de beschreven betrokkenheid van vele – interacterende - partijen), met de daarmee samenhangende business modellen, met efficiencyoverwegingen en met algemeen belang aspecten. Internetserviceproviders vervullen weliswaar een belangrijke spilfunctie, maar zij zijn slechts een van de partijen in

een complexe waardeketen. Het eenzijdig neerleggen van zorgverplichtingen bij internetserviceproviders creëert een onbalans, die enerzijds geen recht doet aan de positie van de providers en anderzijds negatieve effecten met zich meebrengt voor onder meer het aanbieden van diensten en innovatie. Internetserviceproviders zullen immers hun risico's inschatten op basis van hun eigen businessmodel. Laat dat slechts een beperkte risicomarge toe, dan zal men geneigd zijn om risico's uit te sluiten of te mitigeren. Met als consequentie dat diensten die het risico vergroten niet langer toegankelijk zijn voor eindgebruikers of dat nieuwe diensten niet worden ontwikkeld. Efficiency overwegingen zijn eveneens van belang: ogenschijnlijk voor de handliggende oplossingen kunnen bij nadere toetsing niet efficiënt blijken te zijn of tot hoge kosten leiden (dit speelt bijvoorbeeld ten aanzien van filtering of deep packet inspection). Het algemeen belang speelt onder meer een rol wanneer het gaat om het zeker stellen van toegang tot het internet voor iedereen en tegen betaalbare tarieven.

Het belang van een waardeketen georiënteerde benadering krijgt meer en meer aandacht in de literatuur[43], maar wordt eveneens door veel van de geïnterviewden onderschreven. Met name internetserviceproviders zijn kritisch over de mate waarin zij geacht worden zorgplichten te hebben. Zij wijten dit onder meer aan hun hoge zichtbaarheid en de directe relatie die zij hebben met eindgebruikers. Andere partijen in de waardeketen zijn het er in ieder geval over eens dat internetserviceproviders in veel gevallen niet de partij zijn waarop zorgplichten rusten en nemen ook zelf positie, hetgeen bijvoorbeeld zichtbaar is in hun betrokkenheid bij de bestrijding van kinderporno, handhaving van auteursrechten, tegengaan van identiteitsfraude of verkoop van gestolen goederen en bij het bevorderen van internetveiligheid. Het concept van een waardeketenbenadering zou dan ook verdere uitwerking verdienen.

3.3 Positie aanbieders internettoegang

Internetserviceproviders verschaffen eindgebruikers toegang tot het internet en verrichten daarnaast nog allerlei andere taken, zoals het hosten van persoonlijke pagina's websites of het leveren van toegevoegde waardediensten zoals e-mail. Het onderzoek geeft aan dat aan dit onderscheid afdoende belang moet worden toegekend. Als toegangsverschaffers vallen internetserviceproviders sowieso onder het lichte e-commerce regime van 'mere conduit', maar zij claimen ook het 'aan de boodschap geen boodschap'-adagium dat bekend is uit het 'oude' telefoontijdperk en dat werd gebruikt om aan te duiden dat de transporteur niet verantwoordelijk kon worden gehouden voor de inhoud van het getransporteerde.

Als transporteur zijn internetserviceproviders gehouden aan het communicatiegeheim, zo wordt gesteld, en kunnen zij derhalve ook feitelijk geen verantwoordelijkheden dragen met betrekking tot hetgeen internetgebruikers (of dienstenaanbieders) doen op het internet. Er

.[43] OECD (2010); Dommering & Van Eijk (2010); Rand Europe (2008); Ofcom (2008).

zijn toegangsaanbieders die menen dat zij in beginsel gehouden zijn om bijvoorbeeld spam door te laten – immers het verkeer tussen aanbieders en afnemers dient niet gehinderd te worden – maar dat zij op grond van hun contractuele relatie met de eindgebruiker spamfilters toepassen. In dit verband is de vraag relevant waar de bescherming, die verbonden is aan het mere conduit regime van de E-commerce richtlijn, begint en eindigt. Kan een strikte scheiding tussen de internetserviceprovider als aanbieder van toegang worden onderscheiden van het bieden van toegevoegde diensten zoals spamfiltering, dienen dergelijke activiteiten onder mere conduit te worden geschaard, dienen ze als een aparte categorie te worden gezien of gaat om activiteiten die onder de regels voor hosting/caching vallen (of moeten worden gebracht)?

Deels gaat het hier om argumenten die overeenkomen met standpunten die ook spelen bij de discussie over internetneutraliteit. In aanvulling daarop wordt nog naar voren gebracht dat internettoegang meer en meer als een universele dienst is te beschouwen. Aanbieders – ook al staan zij in concurrentie met elkaar – menen dat eindgebruikers 'recht' hebben op internettoegang en dat zij gebruikers bij de toelating in beginsel niet kunnen discrimineren.

3.4 Notice and take down dominant

Samenvattend kan worden geconcludeerd dat notice and take down-systemen bij drie van de vijf thema's (auteursrechten, kinderporno, gestolen goederen) dominant zijn als ordeningsmechanisme. In voorkomende gevallen verplicht regelgeving internetserviceproviders om notice and take down procedures in te stellen en aldus inhoud te geven aan hun zorgverplichtingen. Waar er geen specifieke wettelijke verplichting is geeft het onderzoek aan dat op eigen initiatief notice and take down procedures zijn geïmplementeerd om zo een beroep te kunnen doen op de verlichte aansprakelijkheid met betrekking tot hosting en caching activiteiten.

Maar notice and take down is eveneens een veel voorkomende praktijk buiten de kring van partijen die vallen onder hosting en caching, zoals platform-aanbieders en andere intermediairs (bijvoorbeeld zoekmachines). Zij kunnen zich veelal niet beroepen op een bijzondere rechtsregel (er zijn landen die de bescherming van de e-commerce regels ook hebben uitgebreid naar andere spelers in de waardeketen waaronder platform-aanbieders),[44] maar gebruiken notice and take down om hun algemene civielrechtelijke verantwoordelijkheid in te perken. Door het ontbreken van een verdere juridische inkadering is niet duidelijk in welke mate terecht een vergelijkbaar beroep kan worden gedaan op een verminderde aansprakelijk zoals geregeld ten aanzien van partijen die onder de werking van de E-commerce richtlijn vallen.

[44] Zie Van Hoboken (2009) en Europese Commissie (2003)

'Notice and take down'-procedures zijn reeds onderwerp van uitgebreider onderzoek en evaluatie, zoals in paragraaf 1.3.2 is beschreven, maar verdienen zonder meer verdere aandacht. Daar komt bij dat herziening van de E-commerce richtlijn een van de actiepunten is van Europese digitale agenda.

3.5 Lokale context

De inventarisatie en analyse van nationale regelgeving in combinatie met de interviews geeft aan dat nationale omstandigheden mede bepalend zijn voor de wijze van regulatoire inrichting. Traditioneel kent het Verenigd Koninkrijk een hoog ontwikkeld niveau van zelfregulering. Dit is onder meer terug te vinden in het systeem dat wordt gehanteerd in verband met het bestrijden van kinderporno, dat verder gaat dan alleen een meldsysteem. In Frankrijk ligt de nadruk eerder op regulering via wetgeving. Zelfregulering is duidelijk minder ontwikkeld dan in het Verenigd Koninkrijk. Duitsland neemt een positie in die dichter ligt bij het Verenigd Koninkrijk dan bij Frankrijk. Globaal ingeschat lijkt Nederland een positie in te nemen die tegen de Duitse aanligt. Zelfregulering is aanwezig en werkt, zeker in het geval van kinderporno. De gedragscode notice and take down heeft toegevoegde waarde maar kent ook zwakke kanten, zoals ruime interpretatie-mogelijkheden en het ontbreken van een nalevingsinstrument.

3.6 Handhavingsvraagstukken

Uit de interviews blijkt dat handhaving van het geldende normenstelsel op meerdere kritische factoren stuit. In de eerste plaats is er inzake de strafrechtelijke handhaving een permanente afweging tussen de ernst van de aangelegenheid en de beschikbare middelen. Bij kinderporno is substantiële opsporingscapaciteit aanwezig, maar deze is niet altijd voldoende. Bovendien wordt – al dan niet aanvullend – een beroep gedaan op traditionele opsporingsmethoden, die in voorkomende gevallen even effectief lijken te zijn of afdoende worden geacht. De dilemma's die in dit verband spelen zijn voor wat betreft Nederland al eerder goed in kaart gebracht[45] en uit de interviews komt naar voren dat ook elders wordt geworsteld met vergelijkbare vraagstukken, inclusief afdoende kennis omtrent de technologische aspecten.

In verschillende interviews is het verplicht stellen van filters aan de orde geweest. Er bestaat grote aarzeling ten aanzien van de effectiviteit van filtering, hetgeen ook in de literatuur wordt bevestigd.[46] De filters zijn eenvoudig te omzeilen voor wie dat echt wil. Filters maken hooguit onzichtbaar, maar de wederrechtelijke activiteit wordt er niet door beëindigd. Het gevaar bestaat dat filtering daarmee een excuus wordt voor het niet

[45] Stol e.a. (2008).
[46] o.a. Stol e.a.(2008); Callanan e.a. (2009).

optimaliseren van de bestrijding van de onderliggende illegale activiteiten. Maar ook spelen vragen als: wie is aansprakelijk voor de goede werking van filters, wat zijn de risico's voor underblocking/overblocking/mission creep, wat is de proportionaliteit van het middel, enz.? Deze vragen zijn niet nieuw maar komen telkens opnieuw naar voren bij discussies over filtering. Wat opvalt is dat diverse respondenten (ook aan opsporingszijde) de betrekkelijkheid ervan onderkennen. Anderen zien filtering als een ultimum remedium: indien handhaving stuit op het ontbreken van rechtsmacht, zou filtering als optie inzetbaar kunnen zijn.

De interviews geven verder aan dat er eveneens flinke aarzelingen zijn bij het inzetten van strafrechtelijke handhavingsinstrumenten bij recente wetgeving op het gebied van het auteursrecht. Met name in Frankrijk, waar deze nieuwe wetgeving in een implementatiefase verkeert, worden bij de effectiviteit daarvan kanttekeningen geplaatst. Daarbij wordt onder meer gewezen op het feit dat grote delen van de bevolking worden gecriminaliseerd en dat de regulering een hoge politieke lading heeft. Voorts wordt gewezen op de maatschappelijke weerstand, het opsporingsapparaat zou geheel andere prioriteiten hebben en zou zich anderzijds voor een proportionaliteitsvraag zien gesteld en het gerechtelijk apparaat zou niet over de capaciteit beschikken om een grote hoeveelheid zaken aan te kunnen. Net als elders wordt ook hier de vraag gesteld wiens probleem hier opgelost wordt, waarbij met name op eigen de verantwoordelijkheid van de sector wordt gedoeld inzake het bewaken van de eigen economische belangen, zoals het ontwikkelen van nieuwe businessmodellen. Tot slot is door meerdere partijen de vrees uitgesproken dat 'peer to peer' ondergronds gaat en massaal gebruik gaat maken van encryptie. Hierdoor zou een niet te traceren communicatienetwerk ontstaan waaraan grote delen van de bevolking deelnemen. Het gevaar bestaat dat dit netwerk tevens voor andere zaken gebruikt zal gaan worden dan alleen voor het verspreiden van auteursrechtelijk beschermd materiaal.

Deep packet inspection als handhavingsmethode wordt wel gesuggereerd, maar daar staat ook sterke oppositie tegenover. Internetserviceproviders beroepen zich op het communicatiegeheim en stellen dat er hoge kosten zijn gemoeid met het permanent monitoren van al het internetverkeer. Deskundigen stellen vragen met betrekking tot de proportionaliteit/legitimiteit van deep packet inspection.

Het is van belang dat bij het opleggen van nieuwe regelgeving voldoende aandacht uitgaat naar de proportionaliteit van de voorgestelde maatregelen en de consequenties met betrekking tot de handhaafbaarheid.

3.7 Beantwoording onderzoeksvraag

De onderzoeksvraag richt zich in de eerste plaats op de vormen van zorgplichten die voor internetserviceproviders in de onderzochte landen gelden of worden ontwikkeld, de rol

van de overheid daarbij en de onderliggende beweegredenen voor de gekozen aanpak en daarbij opgedane ervaringen. In de landenstudies komen de diverse deelaspecten van de onderzoeksvraag aan de orde, maar deze worden hier tevens kort samengevat en zijn in de volgende paragraaf in concluderende zin verwoord.

Ten aanzien van de vijf thema's komt naar voren dat de overheden kiezen voor een inzet die gebaseerd is op het gehele palet aan mogelijkheden. Van volledige afzijdigheid van de overheid en het initiatief geheel aan de markt overlaten is nog maar in zeer beperkte mate sprake. Eerder is er een beeld van minder naar meer betrokkenheid, waarbij een sterk accent ligt op vormen van co- of zelfregulering. Europese kaders zijn daarbij van invloed. Deze schrijven expliciete implementatie voor, bij voorbeeld in het geval van internetveiligheid en in het regime van de E-commerce richtlijn. In voorkomende gevallen is daarbij een additionele verantwoordelijkheid in regelgeving neergelegd. Dit doet zich onder meer voor bij het voorschrijven van een notice en take down procedure bij caching of hosting. De richtlijn stelt een dergelijke procedure niet verplicht, alhoewel de invoering ervan een logische consequentie is. Landen kiezen er desalniettemin voor om de procedure te borgen en van een wettelijk kader te voorzien. Dat heeft mede te maken met de wijze waarop nationaal gereguleerd wordt of en hoe men meent afdoende rechtszekerheid te kunnen bieden aan marktpartijen. Bij het thema kinderporno is te zien dat zelf/co-regulering aan de basis ligt van het definiëren van zorgverplichtingen. Waarschijnlijk heeft dit te maken met het feit dat er veel Europese sturing is geweest en het onderwerp kan rekenen op een hoge bereidheid van marktpartijen tot medewerking. Overheden hebben een duidelijk stimulerende rol gehad bij het geldende meldsysteem en geven ook (financiële) ondersteuning. In de regel is men positief over het bestaande stelsel van verantwoordelijkheden van internetserviceproviders met betrekking tot kinderporno. Echter, daar waar het gaat om zaken die van meer ingrijpende aard zijn, zoals filtering, volgt uit het nationaal recht dat een wettelijke basis noodzakelijk is (zie de discussie in Nederland inzake filtering). Maar ook het ingrijpende karakter als zodanig kan met zich meebrengen dat een nadere juridische inkadering wenselijk is, bijvoorbeeld om redenen van rechtszekerheid.

De rol van internetserviceproviders bij het thema auteursrecht is – in twee landen – een goed voorbeeld van zeer ingrijpende overheidsinterventie via regelgeving, waarover dan ook veel discussie is. Het betreft een controversiële materie waar kennelijk co- of zelfregulering geen optie was. Vooralsnog zijn er geen ervaringen met de betreffende regulering omdat deze nog in een implementatiefase verkeert. De vraag is of er bij de gekozen aanpak wellicht niet te voortvarend gehandeld is en of aspecten als de handhaafbaarheid en maatschappelijk draagvlak in afdoende mate zijn meegewogen.

Bij de twee thema's internetveiligheid en de verkoop van gestolen goederen is in het eerste geval sprake van een duidelijk wettelijke inkadering, terwijl die bij de verkoop van gestolen goederen juist ontbreekt. Bij internetveiligheid laat zich dat verklaren door de mate van onduidelijkheid over (of onbekendheid met) wat de betreffende bepaling impliceert. Een

behoefte naar meer (Europese) duiding is zichtbaar. Bij de verkoop van gestolen goederen volgt uit de studie dat dit toch als een vraagstuk wordt gezien dat vooral elders in de waardeketen speelt (op het niveau van platformaanbieders), waardoor er geen speciale rol is toegedicht aan internetserviceproviders.

Uit het onderzoek blijkt dat de gekozen aanpak ten aanzien van een aantal aspecten kritische grenzen in zicht komen. Daar speelt voortschrijdend inzicht en de relevantie van de waardeketen een rol. Ten aanzien van E-commerce is een en ander duidelijk zichtbaar. Er zijn vragen ten aanzien van de reikwijdte van de huidige regelgeving, zowel wat betreft het begrippenkader(zoals de vraag welke partijen aanspraak kunnen maken op een hosting-status) als ten aanzien van de vraag hoe om te gaan met andere spelers in de waardeketen, zoals met platformaanbieders. Bij internetveiligheid geeft de verscherping van de bepaling in het Europese richtlijnenkader en de introductie van een meldplicht nieuwe impulsen voor discussie over enerzijds de plaats van de overheid en het toezicht en anderzijds over de verantwoordelijkheden van internetserviceproviders. Gezien de opdracht die aan lidstaten wordt gegeven zal een actiever betrokkenheid van overheidswege entoezichthouders (in de communicatiesector, maar ook inzake privacy) voor de hand liggen.

3.8 Conclusies

Uit het onderzoek komt een wisselend beeld naar voren, wat er op duidt dat ontwikkelingen – inclusief het zoeken naar verder evenwicht binnen de waardeketen – nog volop in gang zijn. Internetveiligheid, meer in het bijzonder voor zover het de relatie tussen de internetserviceprovider en de eindgebruiker betreft, staat duidelijk nog in de kinderschoenen. Dit betekent niet dat er in de praktijk niets gebeurt, maar er is nog weinig formele inkadering of zelfregulering. Kinderporno daarentegen kent een vrijwel identiek regime in de onderzochte landen, waarbij partijen bereid zijn om vergaande medewerking te verlenen bij de bestrijding ervan. Het (INHOPE) meldsysteem is in alle landen aanwezig op basis van zelfregulering of als uitvloeisel van een wettelijk gedefinieerde zorgverplichting. Terugkerend issue bij het tegengaan van de verspreiding van kinderporno is de positie van filtering. Auteursrecht krijgt veel aandacht en heeft in twee van de onderzochte landen tot aanscherping van de regelgeving geleid, waardoor het mogelijk is om eindgebruikers af te sluiten van internettoegang of deze toegang te beperken. De kritiek op de nieuwe regels is echter groot en de interviews geven aan dat men zeer kritisch is wat betreft de daadwerkelijke handhavingsmogelijkheden. Identiteitsfraude wordt vooral aangepakt in de context van de gevolgen van identiteitsfraude. Het zelfstandig strafbaar stellen van identiteitsfraude (naast de al bestaande mogelijkheden om in de publiekrechtelijke sfeer handhavend op te treden) wordt veelal niet noodzakelijk geacht. De verkoop van gestolen goederen via platform aanbieders (lees: veiling- en verkoopsites e.d.) wordt gezien als de primaire verantwoordelijkheid van de platformaanbieder.

Het wisselende beeld, de nog volop aanwezige dynamiek brengt met zich mee dat het niet mogelijk is om bijvoorbeeld bewezen 'best practices' vast te stellen. Desalniettemin bieden de in het onderzoek verzamelde gegevens interessante informatie.

De onderzoekers komen op grond van het door hen gedane onderzoek tot de volgende conclusies:

1. Naar een waardeketen-benadering
Zorgplichten, zoals in het onderzoek geanalyseerd, kunnen niet gekoppeld worden aan één specifieke partij in de waardeketen tussen informatiedienstenaanbieders en eindgebruikers, maar dienen een gezamenlijke – gebalanceerde – verantwoordelijkheid te zijn van de betrokkenen in de waardeketen. Alleen dan is gewaarborgd dat ongewenste belemmeringen bij de toegang tot het internet worden voorkomen en innovatie niet onder druk komt te staan. Bij de eventuele introductie van nieuwe verplichtingen dient zoveel mogelijk vooraf te worden getoetst wat de effecten ervan zullen zijn op de waardeketen (zoals implicaties voor bedrijfsmodellen en innovatie).

2. Ex ante toetsing effectiviteit en handhaafbaarheid
Vooraf toetsing van (beoogde) juridische interventie met betrekking tot effectiviteit en handhaafbaarheid draagt bij aan het voorkomen van symboolwetgeving en ongewenste (maatschappelijke) effecten.[47]

3. Inzetbaarheid 'notice and take down' -procedures
'Notice and take down'-procedures blijken een breed geaccepteerd mechanisme. De procedures worden niet alleen gehanteerd door internetserviceproviders (in hun hoedanigheid als aanbieder van hosting en caching diensten). Ook andere partijen in de waardeketen, zoals platform-aanbieders, kennen vergelijkbare procedures. Een specifieke juridische grondslag ontbreekt in de meeste onderzochte landen, al zijn er wel initiatieven in de sfeer van zelf- en coregulering. Het verdient aanbeveling om 'notice and take down'-procedures verder in te kaderen, de kring van partijen die er gebruik van kunnen maken nader te definiëren/variëren, alsmede om aan te geven wat de effecten van dergelijke procedures zijn. Vraagstukken rond 'notice and take down', en meer in het algemeen de positie van de E-commerce richtlijn, zijn reeds onderwerp van onderzoek geweest, maar behoeven verdere verdieping. Het is tekenend dat nog geen voorstellen zijn gedaan voor aanpassing van de E-commerce richtlijn, ofschoon die inmiddels wel zijn aangekondigd in het kader van Europese Digitale Agenda

4. Internetveiligheid en privacy verduidelijken
De nieuwe regels inzake internetveiligheid en privacy (artikel 4 van de Europese richtlijn inzake Privacy en de elektronische communicatie) zijn onduidelijk en vragen om verdere precisering wat betreft betekenis en impact. In beginsel ligt hier een taak op Europees

[47] Zie de Duitse discussie over e filtering van kinderporno en hetgeen naar voren komt in de interviews over de implementatie/toepassing van de Franse HADOPI-wetgeving

niveau ten einde te voorkomen dat er te grote verschillen op nationaal niveau optreden. Een nadere afbakening tussen veiligheidsvraagstukken die de relatie internetservice-providers/eindgebruiker raken en veiligheidsvraagstukken die meer liggen op nationaal niveau is wenselijk.

5. Verhoging kennisniveau

De behoefte tot nadere regulering wordt mede gevoed door het ontbreken van voldoende technische en praktische kennis. Kennislacunes blijken juist ten aanzien van de onderzochte problematiek nog volop aanwezig te zijn. Wanneer eindgebruikers, toezichthouders, handhavers en regelgevers hun kennis verder vergroten zal dit kunnen bijdragen aan een verminderde reguleringsdruk. Het belang van educatie wordt breed gedragen.

4 Literatuurlijst

Boer & Grimmius (2009)
L. Boer & T.K. Grimmius, *Melding maken? Internationale quick scan meldplicht gegevensverlies*, onderzoek in opdracht van het Ministerie van Economische Zaken, Research voor beleid, 2009

Chavannes (2007)
R. Chavannes, 'Brein/KPN: het gevaar van een bagatel', *Mediaforum* 2007-6, p. 177.

Callanan e.a. (2009)
C. Callanan, M. Gercke, E. de Marco & H. Dries-Ziekenheiner, *Internet Blocking, balancing cybercrime responses in democratic societies*, studie in opdracht van het Open Society Institute, 2009.

De Cock Buning & Van Eek (2009)
M. de Cock Buning & D. van Eek, 'Aansprakelijkheid van derden bij auteursrechtinbreuk', *IER*, 2009/5, oktober 2009, p. 224-232.

Coupez (2010)
F. Coupez, 'Obligation de notification des failles de sécurité: quand l'Union européenne voit double...', François Coupez, <www.juriscom.net>, 30 januari 2010.

Dommering & Van Eijk (2010)
E.J. Dommering & N.A.N.M. van Eijk, *Convergentie in regulering: Reflecties op elektronische communicatie*, publicatie van het Ministerie van Economische Zaken, 's-Gravenhage, maart 2010.

Dumortier & Somers (2008)
J. Dumortier & G. Somers, *Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software*, Time.lex CVBA, Brussel, 2008.

Van Eeten, Bauer & Tabatabaie (2009)
M. van Eeten, J.M. Bauer & S. Tabatabaie, *Damages from Internet Security, A framework and toolkit for assessing the economic costs of security breaches*, onderzoek in opdracht van OPTA, TU Delft, februari 2009.

Van Eeten, e.a. (2010)
M. van Eeten, J.M. Bauer, Hadi Asghari, Shirin Tabatabaiea, & Dave Rand, *The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data,* http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf

Europese Commissie (2003)
Europese Commissie, *Eerste verslag over de toepassing van Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 200 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("richtlijn inzake elektronische handel")*, COM(2003)702 definitief.

Gercke (2006)
M. Gercke, 'Zugangsprovider im Fadenkreuz der Urheberrechtsinhaber: Eine Untersuchung der urheberrechtlichen Verantwortlichkeit von Downloadportalen und Zugangsprovidem für Musikdownloads', *Computer und Recht* (2006) 22:3, p. 210-216.

Gercke (2009)
M. Gercke, 'Die Entwicklung des Internetstrafrechts im Jahr 2008', *ZUM* (2009), p. 526-538, 528.

Van Hoboken (2009)
J.V.J. van Hoboken, 'Legal Space for Innovative Ordering. On the Need to Update Selection Intermediary Liability in the EU', *International Journal of Communications Law & Policy*, 2009-13, p. 1-21.

Van der Hulst & Neve (2008)
R.C. van der Hulst & R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders*, WODC, 2008.

Elkin-Koren (2006)
N. Elkin-Koren, 'Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic', 9 *N.U. J. Legis. & Pub. Pol'y* 15 (2006).

Kuner e.a. (2009)
C. Kuner, C. Burton, J. Hladjk & O. Proust, *Study on Online Copyright Enforcement and Data Protection in Selected Member States*, Studie in opdracht van de Europese Commissie, Hunton& Williams, 2009.

Van der Meulen (2006)
N. van der Meulen, *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union*, Tilburg: International Victimology Institute Tilburg, 2006

Van der Meulen (2009)
N.S. van der Meulen, 'Identiteitsfraude: de eerste stap, nu nog de rest', *Computerrecht* 229,38, p. 61-64.

OECD (2010)
OECD, *The Economic and Social Role of Internet Intermediaries*, Parijs, april 2010.

Ofcom (2008)
Ofcom, *Ofcom's Response to the Byron Review,* 2008
(http://www.ofcom.org.uk/research/telecoms/reports/byron/).

Rand Europe (2008)
Rand Europe, *Responding to Convergence: Different approaches for Telecommunication regulators*, 2008.

Ringnalda, Elferink & De Cock Buning (2009)
A. Ringnalda, M. Elferink & M. de Cock Buning, *Auteursrechtinbreuk door P2P filesharing, regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*, WODC, 2009

Schellekens, Koops & Teepe (2007)
M.H.M. Schellekens, B.J. Koops & W.G. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg, november 2007.

Stol e.a. (2008)
W.Ph. Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt & A.R. Lodder, *Filteren van kinderporno op internet, Een verkenning van technieken en reguleringen in binnen- en buitenland*, WODC, 2008.

Spindler & Verbiest (2007)
T. Verbiest & G. Spindler, *Study on the Liability of Internet Intermediaries*, studie in opdracht van de Europese Commissie (contract ETD/20-06/IM/E2/69), November 2007.

Stratix (2007)
Stratix Consulting, *Onderzoek inzake Artikel 11.3 Tw, Concept Dreigingsbeeld,* Hilversum, 2007.

TNO/SEO/IVIR (2009)
Ups and downs. Economische en culturele gevolgen van file sharing voor muziek, film en games, onderzoek door een consortium van TNO Informatie- en Communicatietechnologie, SEO Economisch Onderzoek en het Instituut voor Informatierecht, in opdracht van de Ministeries van OCW, EZ en Justitie, januari 2009.

Thoumyre (2008)
Lionel Thoumyre, 'Précisions contrastées sur trois notions clés relatives à la responsabilité des hébergeurs', 35, *Revue Lamy Droit de l'Immatériel*, Février 2008.

Vermissen (2009)
J.A.G. Vermissen, 'Sociale netwerken en privacy', *Privacy & Informatie* 2009-5, p. 233-237.

De Vries e.a. (2007)
U.R.M.Th. de Vries, H. Tigchelaar, M. van der Linden & A.M. Hol, *Identiteitsfraude: een afbakening, een internationale begripsvergelijking en analyse van nationale strafbepalinge*n, WODC/ Universiteit Utrecht, 2007.

Bijlagen

1. Landenstudies

Nederland

Inleiding

I. Bestaande regelgeving

Wettelijk kader

Op grond van de Aanpassingswet richtlijn elektronische handel zijn er diverse bepalingen die de positie van internetserviceproviders met betrekking tot online doorgegeven en opgeslagen gegevens inkaderen.[48] Deze bepalingen bevatten vereisten voor internetserviceproviders die van belang zijn voor de meeste thema's die onderwerp zijn van dit onderzoek en die in volgende paragrafen nader worden besproken. Indien relevant wordt terugverwezen naar dit inleidende deel voor een gedetailleerde beschrijving van deze bepalingen.

Ter uitvoering van de artikelen 12 tot en met 15 van de E-commerce richtlijn, zijn in artikel 6:196c van het Burgerlijk Wetboek (BW) bepalingen neergelegd die onder bepaalde voorwaarden de civielrechtelijke aansprakelijkheid uitsluiten van degenen die 'diensten van de informatiemaatschappij' verrichten die betrekking hebben op het verstrekken van bepaalde informatie, afkomstig van derden die van hun faciliteiten gebruik maken. In de leden 1, 3 en 4 wordt verwezen naar artikel 3:15d lid 3 BW voor een definitie van deze categorie diensten, die vallen onder de werkingssfeer van de bepalingen. Belangrijkste eis in deze definitie is dat enige economische activiteit wordt verricht met een dergelijke dienst. De reikwijdte van het begrip economische activiteit in deze zin omvat in ieder geval meer dan alleen directe online transacties. Verder moet het gaan om diensten die 'op afstand' worden gebruikt, dat wil zeggen in geografische zin, op elektronische wijze via een systeem van opslag en verwerking van gegevens, en op individueel verzoek.

De bepalingen in artikel 6:196c BW zijn van toepassing voor zover deze tussenpersonen publiekelijk beschikbare informatie doorgeven of opslaan via hun faciliteiten. De voorwaarden, op limitatieve wijze door deze bepalingen vastgesteld, maken duidelijk van welke maatregelen de bedoelde dienstenaanbieders zich moeten bedienen of onthouden,

[48] Aanpassingswet richtlijn inzake elektronische handel, *Stb.* 2004, 210; *Kamerstukken II* 2001-02, 28 197

om zich vrij te stellen van aansprakelijkheid voor bepaalde informatie afkomstig van hun abonnees en gebruikers. De bepalingen bevatten een aan de E-commerce richtlijn ontleend onderscheid tussen mere conduit, caching en hosting activiteiten. De dienstenaanbieders die deze activiteiten verrichten kunnen in het algemeen enkel een beroep doen op de uitsluiting van aansprakelijkheid, wanneer kan worden gezegd dat zij op geen enkele wijze betrokken zijn bij de verrichte activiteiten anders dan door het beschikbaar stellen van de technische middelen die de betreffende communicatie vergemakkelijken.

Het artikel bepaalt in overeenstemming met artikel 15 lid 2 van de E-commerce richtlijn uitdrukkelijk, in lid 5, dat de bepalingen niet de mogelijkheid uitsluiten van het verkrijgen van een rechterlijk verbod of bevel om het verspreiden van bepaalde informatie te beëindigen. De bepalingen bevatten geen algemene verplichting om toe te zien op de informatie die de dienstenaanbieders doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden. Er is verder geen verplichting om de bevoegde autoriteiten onverwijld in kennis te stellen van vermeende onwettige activiteiten of informatie door afnemers van de genoemde diensten, hoewel artikel 15 lid 2 van de E-commerce richtlijn een dergelijke verplichting als mogelijkheid noemt.

Artikel 6:196c lid 1 BW gaat over mere conduit activiteiten. Mere conduit heeft betrekking op het doorgeven van van een ander afkomstige informatie of op het verschaffen van toegang tot een communicatienetwerk. In lid 2 van het artikel wordt bepaald dat de geautomatiseerde, tussentijdse en tijdelijke opslag van de doorgegeven informatie, voor zover deze opslag uitsluitend geschiedt ten behoeve van het doorgeven van die informatie en de duur van deze opslag niet langer is dan daarvoor redelijkerwijs noodzakelijk is, valt onder 'doorgeven' en 'het verschaffen van toegang', zoals vermeld in lid 1. Zolang internetserviceproviders geen informatie op hun servers cachen of hosten, in de zin van lid 3 respectievelijk lid 4 van het artikel, zijn zij ingevolge deze bepaling tot geen enkele maatregel gehouden om aansprakelijkheid voor de doorgegeven informatie te voorkomen, op voorwaarde dat zij niet het initiatief nemen tot het doorgeven van de informatie, niet degenen zijn die bepalen aan wie de informatie wordt doorgegeven, en zij de doorgegeven informatie niet hebben geselecteerd of gewijzigd.

Artikel 6:196c lid 3 BW heeft betrekking op caching activiteiten, in de zin van het geautomatiseerd, tussentijds en tijdelijk opslaan van van een ander afkomstige informatie voor zover het opslaan enkel geschiedt om het later doorgeven van die informatie aan anderen op hun verzoek doeltreffender te maken. Wanneer internetserviceproviders deze activiteit verrichten, moet aan vijf cumulatieve vereisten worden voldaan om een beroep op de uitsluiting van aansprakelijkheid uit deze bepaling te kunnen doen. In de eerste plaats mogen ze de informatie niet wijzigen. Ten tweede moeten ze de voorwaarden voor toegang tot de informatie in acht nemen. Ten derde, moeten ze de in de bedrijfstak geldende of gebruikelijke regels betreffende de bijwerking van de informatie naleven. Ten vierde, moet de in de bedrijfstak geldende of gebruikelijke technologie voor het verkrijgen van gegevens

over het gebruik van de informatie ongewijzigd blijven. Ten vijfde, moeten ze prompt de nodige maatregelen nemen om de informatie te verwijderen of de toegang daartoe onmogelijk te maken, zodra ze weten dat de informatie is verwijderd van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe onmogelijk is gemaakt, of dat een bevoegde autoriteit heeft bevolen de informatie te verwijderen van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe heeft verboden.

Artikel 6:196c lid 4 BW is van toepassing op hosting activiteiten. Het gaat om dienstenaanbieders die vallen onder het toepassingsgebied van artikel 6:196c BW (daarmee verwijzend naar artikel 3:15 lid3 BW), die diensten verrichten bestaande uit het op verzoek opslaan van informatie die van een ander afkomstig is. Deze tussenpersonen moeten maatregelen nemen om hun aansprakelijkheid uit te sluiten indien zij daadwerkelijk kennis hebben van het onrechtmatige karakter van een activiteit of van informatie, of, wanneer het een civiele vordering tot schadevergoeding betreft, redelijkerwijs behoren te weten van de activiteit of informatie met een onrechtmatig karakter. Voor deze kennis, is een kennisgeving op zichzelf niet genoeg. Het moet betrekking hebben op 'onmiskenbaar onrechtmatige' activiteiten of informatie. Het kan de aard, de kwaliteit of de status van de informatie zijn waardoor zij onrechtmatig of strafbaar is. Onder deze omstandigheden, moeten dienstenaanbieders die hosten prompt de informatie verwijderen of de toegang daartoe onmogelijk maken.

Naast de verminderde civielrechtelijke aansprakelijkheid zoals vormgegeven door de bepalingen in artikel 6:196c BW, bevat artikel 54a van het Wetboek van Strafrecht (Sr) een vrijwaring van strafrechtelijke vervolging onder bepaalde voorwaarden. Artikel 125o Wetboek van Strafvordering (Sv) voorziet in een bevoegdheid om informatie in een 'geautomatiseerd werk' ontoegankelijk te maken. Beide artikelen worden expliciet genoemd in de memorie van toelichting bij de Aanpassingswet richtlijn elektronische handel, als de juridische grondslag voor de implementatie van de bepalingen over verminderde aansprakelijkheid voor tussenpersonen uit de artikelen 12 tot en met 15 van de E-commerce richtlijn, in het kader van strafrechtelijke procedures.

Artikel 54a Sr bepaalt dat tussenpersonen die telecommunicatiediensten verlenen, bestaande uit de doorgifte of opslag van gegevens die van een ander afkomstig zijn, niet als zodanig zullen worden vervolgd voor deze activiteiten, indien zij voldoen aan een bevel van een officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door een rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hen kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Artikel 125o Sv voorziet in de mogelijkheid voor opsporingsinstanties om gegevens die bij een doorzoeking in een geautomatiseerd werk worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, ontoegankelijk te maken voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van

nieuwe strafbare feiten. Het besluit om deze gegevens ontoegankelijk te maken behoeft toestemming van een officier van justitie of een rechter-commissaris, afhankelijk van de fase waarin het onderzoek zich bevindt (lid 1), en moet als doel hebben dat de beheerder van het geautomatiseerde werk of derden niet verder van die gegevens kennisnemen of ervan gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens (lid 2). Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen, moeten de geblokkeerde gegevens weer ter beschikking worden gesteld aan de beheerder van het geautomatiseerde werk na toestemming van een officier van justitie of een rechter-commissaris.

Overige regulering

De maatregelen die internetserviceproviders kunnen nemen om aansprakelijkheid of vervolging te voorkomen, zoals hierboven beschreven, impliceren de aanwezigheid van zogenaamde notice and take down procedures. Er zijn geen wettelijk vormgegeven notice and take down procedures in Nederland om verdere invulling te geven aan de vereisten van de hierboven beschreven wettelijke bepalingen.

De Gedragscode Notice-and-Take-Down geeft algemene richtlijnen voor notice and take down procedures, bedoeld om aanwijzingen te geven voor de ontwikkeling van maatregelen door tussenpersonen die een 'openbare telecommunicatiedienst op het internet' verzorgen (artikel 1b) en die te maken hebben met klachten over onrechtmatige en/of strafbare inhoud in de online-omgeving. De gedragscode is geïnitieerd door de Nederlandse overheid, internetbedrijven en belangengroepen.[49] De eerste versie van de code werd gecoördineerd door de Nationale Infrastructuur ter bestrijding van Cybercrime (NICC), die wordt ondersteund vanuit het Ministerie van Economische Zaken. De initiatiefnemers onderhouden de code op een continue basis, momenteel gecoördineerd door het Platform voor de InformatieSamenleving (ECP-EPN), een platform voor onderhandelingen tussen overheidsinstanties en particuliere bedrijven. Het ECP-EPN is ook gastheer van het Platform Internetveiligheid, dat is bedoeld als een discussieforum voor de overheid en private partijen om initiatieven te ontwikkelen om de veiligheid op internet te verhogen.

De richtlijnen in de Gedragscode Notice-and-Take-Down zijn onderverdeeld in artikelen waarbij een memorie van toelichting is toegevoegd. De artikelen beschrijven hoe de bedoelde tussenpersonen kunnen omgaan met (geldige) klachten over onrechtmatige en strafbare inhoud op internet, zoals de distributie van illegale goederen of kinderporno. Een speciale vermelding in de gedragscode introduceert 'ongewenste' inhoud als een aparte categorie ten aanzien waarvan wordt voorgesteld dat tussenpersonen zelf kunnen beslissen welke soorten informatie eronder vallen. Het is aan hen om te bepalen of ze daarmee op

[49] Zie http://www.ecp-epn.nl/werkgroep-notice-and-takedown voor een lijst van initiatiefnemers en partners van de Gedragscode Notice-and-Take-Down.

dezelfde wijze willen omgaan als met onrechtmatige en strafbare inhoud. In artikel 3b wordt de mogelijkheid genoemd dat tussenpersonen in hun gebruiksvoorwaarden de criteria vermelden wanneer er sprake is van ongewenste inhoud. De gedragscode geeft verder richtlijnen over hoe beoordeeld kan worden of een klacht gegrond is of niet, en welke stappen moeten worden genomen tijdens de fase waarin de tussenpersoon zou hebben besloten dat het verwijderen van het materiaal de juiste reactie is op een klacht. Artikel 1c stelt dat de gedragscode niet van toepassing is wanneer voor tussenpersonen, gebaseerd op recht en rechtspraak, andere verplichtingen gelden. In de memorie van toelichting wordt toegelicht dat de gedragscode geen nieuwe wettelijke verplichtingen schept. De toelichting verwijst daarbij naar de bepalingen over verminderde aansprakelijkheid voor tussenpersonen van artikel 6:196c BW.

Verschillende Nederlandse internetserviceproviders, waaronder de grootste, hebben beleidsregels uitgevaardigd over de notice and take down procedure die zij gebruiken.[50]

II. Toepassing bestaande regelgeving

Wettelijk kader

De memorie van toelichting bij artikel 6:196c BW bepaalt dat nadere regels gesteld kunnen worden, bijvoorbeeld dat voorwaarden met betrekking tot het verwijderen van een website, redelijk en subsidiair moeten zijn, en evenredig gelet op de kosten en de technische en personele eisen voor de internetserviceprovider of andere dienstenaanbieders.[51] Hoewel het duidelijk is dat de bepalingen van artikel 6:196c BW een bepaalde vorm van notice and take down procedures vereisen van de dienstenaanbieders die daarin worden genoemd, is de nadere regulering daarvan tot nu toe bewust overgelaten aan zelfregulering. Er zijn geen wettelijke eisen over bijvoorbeeld de wijze waarop geoordeeld moet worden over de proportionaliteit van de gevraagde maatregelen.

In de rechtszaak *Lycos/Pessers*, over een anonieme publicatie op een website die volgens Pessers onrechtmatig was aangezien het een valse beschuldiging betrof, is een nieuw zorgvuldigheidsvereiste met eigen voorwaarden geformuleerd voor tussenpersonen zoals internetserviceproviders, als het gaat om verzoeken voor afgite van naam-, adres- en

---

[50] Bijvoorbeeld: KPN heft de 'Klachtenprocedure Internet', zie: http://www.kpn.com/prive/service/veiligheid /abuse/welke-incidenten.htm; UPC heeft de 'Regeling Notice & Takedown', zie: http://www.upc.nl/pdf/upc_internet_veiliginternet notice_&_takedown.pdf; SIDN heeft de 'Notice-and-Take-Down-procedure voor .nl-domeinnamen', zie: http://www.sidn.nl/ace.php/p,727,6106,2118423720,021009_-_Notice-and-Take-Down-procedure_voor_nl-domeinnamen_pdf; XS4all hanteert sinds 2007 beleidsregels voor notice and take down procedures, die van invloed zijn geweest op de ontwikkeling van de Gedragscode Notice-And-Take-Down. Zie: http://www.xs4all.nl/overxs4all/contact /media/beleidsregels_klachten.pdf

[51] *Kamerstukken II* 2001-02, 29197, nr. 3, p. 51.

woonplaatsgegevens (NAW-gegevens) van websitehouders.[52] De Hoge Raad oordeelde dat de beoordelingsmaatstaf die het Gerechtshof Amsterdam had geformuleerd, gepast is om voor serviceproviders de noodzaak te kunnen evalueren van verstrekking op verzoek van identificatiegegevens van aanbieders van vermeend onrechtmatige inhoud. Een tussenpersoon moet dergelijke identificerende gegevens verstrekken om aan de vereiste zorgvuldigheid in het maatschappelijk verkeer te voldoen 1) wanneer de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, voldoende aannemelijk is, 2) de derde een reëel belang heeft 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, en 4) de afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) meebrengt mee dat het belang van de derde behoort te prevaleren.

De E-commerce richtlijn heeft de vraag of, en onder welke voorwaarden, dienstenaanbieders moeten reageren op verzoeken voor NAW-gegevens van civiele partijen opengelaten. Volgens de Nederlandse regering voldoen de normen van de *Lycos/Pessers* zaak, gezien in het licht van het arrest van het Hof van Justitie van de Europese Unie in de zaak *Promusicae/Telefónica de Espaáa SAU*, aan de in dat arrest gestelde eisen aan dergelijke zorgvuldigheidsverplichtingen.[53]

Rechtspraak over vermeende lasterlijke informatie op websites, laat zien dat er eveneens vraagstukken spelen omtrent artikel 54a Sr. Een van deze rechtszaken betrof de situatie waarin een rechter-commissaris had geweigerd een openbare aanklager te machtigen om de Nederlandse dienstenaanbieder Budget Webhosting te bevelen inhoud van haar servers te verwijderen. De officier van justitie heeft toen alsnog een notice and take down bevel tegen Budget Webhosting uitgevaardigd, dat de dienstenaanbieder echter niet heeft opgevolgd vanwege het ontbreken van de machtiging van de onderzoeksrechter. De officier van justitie stelde voor de rechtbank dat de situatie onbevredigend zou zijn als er geen verwijderingsbevel mogelijk zou zijn. Er wordt namelijk geen echte evaluatie van de vermeende onrechtmatige inhoud door de onderzoeksrechter uitgevoerd en de beslissing van de onderzoeksrechter kan niet aan rechterlijke toetsing worden onderworpen. De rechter geeft aan dat hier een taak ligt voor de wetgever en niet voor de rechterlijke macht. Het openbaar ministerie had derhalve onwettelijk gehandeld.[54]

Overige regulering

De E-commerce richtlijn, bijvoorbeeld in overweging 40, moedigt de lidstaten aan om co/zelfregulering te stimuleren. De Nederlandse regering heeft dit uitgangspunt

[52] Hoge Raad 25 november 2005, *Mediaforum* 2006-1, nr. 1 met noot A.H. Ekker, Lycos Netherlands B.V. versus A.B.M. Pessers.
[53] *Kamerstukken II* 2007-2008, 29838, nr. 7, p. 2-3. Zie ook: *Kamerstukken II* 2007-08, 28684, nr. 133, p. 2-3.
[54] Rechtbank Assen 24 november 2009, *LJN* BK4226 (onwettelijke vervolging Budget webhosting). Zie ook: Gerechtshof Leeuwarden 20 april 2009, *LJN* BI1643 en BI1645.

onderschreven en de ontwikkeling van procedures voor de afwikkeling van meldingen over onrechtmatige activiteiten en informatie bewust overgelaten aan co-regulering en vrijwillige zelfregulerende maatregelen.[55]

Er is geen officiële lijst van alle gebruikers van de Gedragscode Notice-and-Take-Down. Bedrijven en tussenpersonen die zich conformeren aan deze gedragscode, moeten dat zelf kenbaar maken. Implementatie en naleving van de gedragscode is vrijwillig. Er is geen mogelijkheid, zoals in de memorie van toelichting in de code uitdrukkelijk is bepaald, de naleving ervan formeel af te dwingen.

De gedragscode, geïnspireerd door de beschreven Lycos/Pessers-zaak, noemt in artikel 6c de mogelijkheid voor tussenpersonen om te beslissen of NAW-gegevens van inhoudsaanbieders aan de melder van vermeende onrechtmatige inhoud worden verstrekt. In de toelichting worden de normen vermeld die in een dergelijk geval leidend moeten zijn voor de beoordeling van belangen, zoals ontwikkeld in de Nederlandse jurisprudentie. In de toelichting wordt verder opgemerkt dat er geen wettelijke verplichting voor tussenpersonen bestaat om over dergelijke contactgegevens van hun gebruikers en abonnees te beschikken. In de gedragscode zijn geen richtlijnen opgenomen over hoe te reageren wanneer de evaluatie door een tussenpersoon van het onrechtmatige of strafbare karakter van bepaalde inhoud wordt bestreden en/of gecorrigeerd, bijvoorbeeld door een rechter op verzoek van de oorspronkelijke inhoudsaanbieder. Dit kan leiden tot de noodzaak om bepaalde inhoud alsnog te laten staan of terug te zetten. Artikel 4a juncto artikel 5a van de gedragscode impliceert, volgens de memorie van toelichting, dat wanneer een melding formeel wordt gedaan door een officier van justitie, de tussenpersoon de verplichting heeft hieraan te voldoen zonder een aparte evaluatie van het strafbare karakter van de gemelde inhoud. Er wordt in de toelichting vastgesteld dat in dat geval een dergelijke evaluatie al door een bevoegde instantie is gedaan.

III. Ontwikkelingen

Het Ministerie van Justitie heeft aangekondigd dat een van de belangrijkste elementen van het huidige beleid ter bestrijding van illegale inhoud op het internet, de ontwikkeling is van juridische instrumenten om een grondslag te bieden voor de overheid om de verwijdering van dergelijke inhoud door tussenpersonen te bevelen. De huidige status van artikel 54a Sr en artikel 125o Sv zal worden geëvalueerd.[56]

[55] *Kamerstukken II* 2001-02, 28 197, nr. 3, p. 26. Zie ook: *Kamerstukken II* 2007-08, 28684, nr. 133, p. 14.
[56] *Kamerstukken II* 2007-08, 28684, nr. 133, p. 2 en 14.

Internetveiligheid

I. Bestaande regelgeving

Wettelijk kader

Ter implementatie van artikel 4 van de richtlijn Privacy en elektronische communicatie, bevat artikel 11.3 van de *Telecommunicatiewet* (Tw) een aantal zorgplichten voor aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten.

Dit artikel verwijst naar artikel 11.2 Tw waarin dit soort aanbieders expliciet wordt genoemd. De Nederlandse regering vond het nodig om beide soorten aanbieders onder de reikwijdte van artikel 11.3 Tw te laten vallen, omdat deze netwerken en diensten nauw met elkaar verbonden zijn.[57] De definitie van deze categorieën netwerken en diensten in de Telecommunicatiewet heeft betrekking op bijvoorbeeld internetserviceproviders en aanbieders van mobiele communicatie via telecommunicatienetwerken. Internetproviders die informatiediensten aanbieden via elektronische communicatiediensten, bijvoorbeeld in de vorm van resellers of aanbieders van 'over the top' (OTT)diensten zoals webmail, vallen buiten de definitie.[58]

Artikel 11.2 Tw bevat een algemene zorgplicht voor de bescherming van persoonsgegevens in verband met de privacy van abonnees of gebruikers van netwerken of diensten. Het artikel verwijst naar de *Wet Bescherming Persoonsgegevens* (Wbp) als het algemene wettelijke kader voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.[59]

Artikel 11.3 lid 1 Tw bepaalt dat de bedoelde aanbieders 'passende' technische en organisatorische maatregelen moeten nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. Het artikellid verduidelijkt dat 'passende' impliceert dat het niveau van deze maatregelen in verhouding moet staan tot het betreffende risico, rekening houdend met de huidige stand van technische ontwikkelingen en met de kosten die nodig zijn om deze technieken toe te passen. De maatregelen moeten worden genomen in het algemeen belang van de bescherming van persoonsgegevens en in het belang van de privacy van abonnees en gebruikers.

---

[57] *Kamerstukken II* 1996-1997, 25533, nr. 3, p. 71 en 119.
[58] *Kamerstukken II* 2002-2003, 28 851, nr. 3, p. 89.
[59] Artikel 13 Wbp bevat een vergelijkbare verplichting als artikel 11.2 Tw. Een 'verantwoordelijke' moet passende technische en organisatorische maatregelen ten uitvoer leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Art 11.3 lid 2 Tw voegt een plicht toe om abonnees te informeren over bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst. Zij zijn ook gehouden om de abonnees te informeren over de mogelijke maatregelen om deze risico's tegen te gaan, en over de verwachte kosten die verbonden zijn aan dergelijke maatregelen. De memorie van toelichting bij art 11.3 lid 2 Tw, noemt encryptietechnieken en fire-walls als mogelijke maatregelen waarover abonnees geïnformeerd kunnen worden.[60]

De Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) is de autoriteit om op de bepalingen van artikel 11.3 Tw toezicht te houden (zie artikel 15.1 lid 3 Tw) en deze te handhaven (zie voor de mogelijkheden voor sancties, artikel 15.2 lid 2 en artikel 15.4 lid 4 Tw).

Overige regulering

Op grond van artikel 18.8 Tw kan de Minister van Economische Zaken met betrekking tot de veiligheid en de beveiliging van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten regels stellen inzake technische en organisatorische eisen die aan de aanbieders kunnen worden gesteld. Het gaat om dezelfde aanbieders als in artikel 11.3 Tw. In tegenstelling tot wat is bepaald in artikel 11.3 Tw, hoeven deze regels niet alleen betrekking te hebben op de bescherming van persoonsgegevens en persoonlijke levenssfeer van abonnees en gebruikers. Op dit moment is geen nadere invulling gegeven aan de bepaling.

OPTA heeft beleidsregels gepubliceerd met betrekking tot de plicht om abonnees te informeren zoals beschreven in artikel 11.3 lid 2 Tw. Deze regels geven aan welke risico's binnen deze zorgplicht vallen, wat de mogelijkheden zijn voor de aanbieders om hun gebruikers en abonnees te informeren, welk wettelijke kader OPTA de bevoegdheid geeft om op de zorgplicht toe te zien en welke sancties OPTA gepast acht indien de zorgplicht niet voldoende wordt nageleefd.[61]

Overigens kan nog vermeld worden dat een aantal grote internetserviceproviders in augustus 2009 een convenant heeft gesloten over maatregelen tegen botnets.[62] Daarin is de intentie neergelegd om informatie over botnets uit te wisselen. Ook is de bedoeling om gebruikers te helpen bij het opschonen van hun computers en bij het herstellen van de internetverbinding.

---

[60] *Kamerstukken II* 2002-03, 28851, nr. 3, p. 153-154.

[61] 'Beleidsregels informatieplicht voor aanbieders over internetveiligheid', 2009, OPTA/ACNB/2008/ 202938, http://www.opta.nl/nl/actueel/alle-publicaties/ publicatie/?id=2838.

[62] http://www.xs4all.nl/nieuws/bericht.php?msect=nieuws&id=1055&taal=nl

II. Toepassing bestaande regelgeving

Wettelijk kader

Op parlementair niveau is de vraag gesteld of artikel 11.3 Tw een inspanningsverplichting of een resultaatsverplichting inhoudt. Het eerste lid van het wetsartikel lijkt wat speelruimte te bieden, aangezien het alleen om 'passende' maatregelen gaat, iets wat nadere afweging vereist. Het tweede lid bevat een verplichting om te informeren, zij het met een beperking tot 'bijzondere risico's'.[63]

In 2006 heeft de OPTA 'project 11.3 Telecommunicatiewet' gestart om nader invulling te geven aan de zorgplichten, zoals beschreven in artikel 11.3 Tw. In een extern rapport zijn eerst huidige en toekomstige gevaren en bedreigingen op het internet in kaart gebracht.[64] Het doel daarvan was om duidelijkheid te verkrijgen ten aanzien van de vraag hoe ver de in artikel 11.3 Tw genoemde zorgplichten moeten reiken. Inzicht in de gevaren en bedreigingen die te vinden zijn op het internet, zou helpen om na te gaan welke maatregelen in verband met de veiligheid 'passend' zijn in de terminologie van artikel 11.3 lid 1 Tw. Het rapport bevat vervolgens een overzicht van de resultaten uit de interviews samen met een aantal voorstellen voor beleidsregels in concept.

Mede op basis van de studie heeft OPTA vervolgens drie ontwikkeltrajecten ingezet, die samen de door artikel 11.3 Tw geregelde totale zorgplicht omvatten: a) een beveiligingsplicht, zoals beschreven door artikel 11.3 lid 1 Tw, met betrekking tot de algemene veiligheid van het internet die moet worden beschermd door 'passende' maatregelen; b) een informatieplicht om abonnees te informeren over bijzondere bedreigingen voor de veiligheid, en over maatregelen om deze bedreigingen te bestrijden, zoals beschreven door artikel 11.3 lid 2 Tw en c) de bestrijding van botnets.

Na een consultatieronde in 2007, concludeerde OPTA dat er te veel weerstand bestond tegen beleidsregels met betrekking tot de beveiligingsplicht. OPTA besloot derhalve af te zien van dergelijke regels, mede omdat er bij de marktpartijen een algemene intentie leek te bestaan om tot de ontwikkeling van een keurmerk te komen. Dit keurmerk zou consumenten moeten informeren over de mate van beveiliging en veiligheid die te verwachten is bij het gebruik van de diensten van een bepaalde provider.[65] Uiteindelijk zijn de betrokken internetserviceproviders niet tot overeenstemming gekomen over een

[63] *Kamerstukken II* 1997-1998, 25 533, nr. 5, p. 126.
[64] Stratix (2007)
[65] 'Zorgplicht internetaanbieders', 2008, OPTA/ACNB/2008/201166, http://www.opta.nl/nl/actueel /alle-publicaties/ publicatie/?id=2591.

dergelijk keurmerk. De OPTA heeft in 2008 geconcludeerd dat een keurmerk alleen effectief zou zijn met brede steun, die op dat moment ontbrak.[66]

Botnets genieten speciale aandacht, omdat bestrijding hiervan volgens OPTA veel zou kunnen toevoegen aan de veiligheid van netwerken en diensten.[67] Het is de vraag of de bestrijding van botnets onder de werkingssfeer van artikel 11.3 Tw kan vallen, aangezien daarin wordt verwezen naar het algemeen belang van de bescherming van persoonsgegevens en van de privacy van abonnees en gebruikers. In het algemeen lijkt de bestrijding van botnets zowel door OPTA als internetserviceproviders te worden benaderd als een zorgplicht. Zoals aangegeven hebben marktpartijen een convenant gesloten over de bestrijding van botnets. Passende maatregelen zijn ontwikkeld door middel van onderlinge afspraken tussen internetserviceproviders, zoals het convenant dat in dit deel onder 'overige maatregelen' wordt besproken.

In het algemeen is er een vraag over verdeling van rechtsmacht in dit gebied. Er is samenwerking met de KLPD, die wordt geregeld door een convenant tussen OPTA en de KLPD. Het protocol regelt vooral de mogelijkheden om informatie en bevindingen over de bestrijding van botnets uit te wisselen.[68] De KLPD kan actie ondernemen tegen botnets voor zover de verspreiding van malware deel uitmaakt van strafbare feiten in het Wetboek van Strafrecht.[69] Anders zijn bestuursrechtelijke maatregelen door OPTA mogelijk. Een betrokken internetserviceprovider zou kunnen worden aangepakt als medepleger van de overtreding van het verbod op de verspreiding van malware.[70]

Na de beslissing om af te zien van de beleidsregels ten aanzien van de beveiligingsplicht, heeft de OPTA zich gericht op de informatieplicht. Er is in eerste instantie een nulmeting uitgevoerd. Geconcludeerd is dat er voldoende aan deze verplichting werd gedaan. OPTA heeft het aan de bedrijven zelf overgelaten om vorm te geven aan hun taken. Er is nog geen nieuw evaluatiemoment voorzien. In januari 2009 heeft OPTA beleidsregels vastgesteld met betrekking tot de informatieplicht (zie hierna).

OPTA heeft aangegeven in het algemeen actief te willen bijdragen aan een structureel overleg in Nederland tussen alle bij het internet betrokken partijen over onderwerpen die raken aan de veiligheid en ontwikkeling van het internet in Nederland.[71]

---

[66] 'Vervolg zorgplicht internetaanbieders', 2008, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2718.

[67] S*upra* noten 58 en 59.

[68] 'Samenwerkingsprotocol OPTA-KLPD', 2007, OPTA/TN/2007/201789, http://www.opta.nl/nl/actueel/ alle-publicaties/publicatie/?id=2401.

[69] De artikelen 138a, 138b, 161sexies en 161septies, 350a en 350b Sr worden in het protocol genoemd.

[70] De Nederlandse internetprovider Mega Provider heeft van de OPTA een last onder dwangsom opgelegd gekregen vanwege het faciliteren van spam via haar e-mailservice: 'Last onder dwangsom Megaprovider B.V.', 2006, OPTA/IPB/2006/202031, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2033.

[71] *Supra* noot 57.

Overige regulering

Het meest voorkomende argument van de door OPTA geconsulteerde internetserviceproviders tegen de door OPTA voorgestelde beleidsregels over de zorgplicht ten aanzien van veiligheid (artikel 11.3 lid 1 Tw) is dat het te verwachten is dat dergelijke regels niet goed up-to-date kunnen blijven gezien de manier waarop de internettechnologie evolueert.

OPTA stimuleert zelfregulering, zoals het voorstel van de internetserviceproviders om een keurmerk te ontwikkelen, of het idee om 'best practices' te ontwikkelen, maar wil eerst de inhoud van de zorgplicht, geregeld door artikel 11.3 lid 1 Tw, verder bespreken met de Staatssecretaris van Economische Zaken.

Zoals eerder aangegeven bepaalt het tussen internetserviceproviders gesloten convenant met betrekking tot de bestrijding van botnets, dat informatie over botnets moet worden uitgewisseld tussen de aanbieders. Verder moeten gebruikers worden geholpen om hun computers te reinigen en om ze opnieuw te verbinden. Het valt te verwachten dat de mate van ondersteuning varieert, gezien de verschillen in businessmodellen van de internetserviceproviders.

III. Ontwikkelingen

'Project 11.3 Telecommunicatiewet' is deels afgesloten met de conclusie dat OPTA nader overleg dient te voeren met het Ministerie van Economische Zaken. Het is niet bekend of dit overleg is opgestart. Ook is niet duidelijk of de eerdere concept-beleidsregels verder ontwikkeld zullen worden.

Op parlementair niveau is de vraag gesteld of een plicht om te rapporteren over het verlies van persoonlijke gegevens als gevolg van een inbreuk op de beveiliging, zowel voor vitale overheidsdiensten als particuliere ondernemingen, zou kunnen bijdragen tot een betere bescherming van de persoonlijke levenssfeer en van opgeslagen gerelateerde informatie.[72] Een dergelijke rapportageplicht is in verband hiermee in een aantal landen in de wereld onderzocht.[73] Deze vraag werd ook gesteld tijdens de onderhandelingen over de herziening van de richtlijn Privacy en elektronische communicatie. De Nederlandse regering heeft aangegeven dat er een verplichting is als gevolg van deze herziening om een meldplicht ten aanzien van verlies van persoonlijke gegevens voor aanbieders van elektronische netwerken en diensten te implementeren. Het kabinet heeft sympathie geuit voor het voorstel van het Europees Parlement om de meldplicht te verbreden naar 'diensten van de informatiemaatschappij', zoals banken en online winkels.[74]

---

[72] *Kamerstukken II* 2007-08, 29 668 en 26 643, nr. 22, p. 1.
[73] Boer & Grimmius (2009)
[74] *Kamerstukken II* 2008-09, 26 643, nr. 138, p. 1.

Kinderporno

I. Bestaande regelgeving

Wettelijk kader

Het bezit, de distributie en het beschikbaar stellen van een afbeelding van of een gegevensdrager met een afbeelding van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, is strafbaar op grond van artikel 240b van het *Wetboek van Strafrecht* (Sr). Ook het zichzelf verschaffen van toegang tot een dergelijk afbeelding door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst, wordt strafbaar gesteld in hetzelfde artikel.

Volgens de bepalingen van artikel 6:196c van het *Burgerlijk Wetboek* (BW) geldt een verminderde aansprakelijkheid voor 'aanbieders van diensten van de informatiemaatschappij' in verband met het aanbieden van informatie, die door derden op hun faciliteiten zijn geplaatst. Zoals hierboven besproken in het inleidende deel van deze paragraaf over Nederland, schept artikel 6:196c BW alleen verminderde aansprakelijkheid wanneer voldaan wordt aan bepaalde voorwaarden.

Overige regulering

De al eerder genoemde Gedragscode Notice-and-Take-Down geeft algemene richtlijnen voor notice and take down procedures, die ook van toepassing zijn in het geval van kinderporno.

Specifiek met betrekking tot kinderpornografie, is het Meldpunt Kinderporno op Internet opgericht. [75] Het Meldpunt is onderdeel in het netwerk van INHOPE. Het is opgezet door een aantal internetserviceproviders en individuele internetgebruikers, en opereert als de enige partij naast de Nederlandse politie onder erkenning van het Ministerie van Justitie en de Europese Commissie. In de laatste elf jaar heeft het meldpunt meer dan 40.000 meldingen ontvangen. Deze kunnen rechtstreeks afkomstig zijn van individuele gebruikers of van bijvoorbeeld internetserviceproviders. Het Meldpunt controleert of het materiaal strafbaar is. Als het materiaal strafbaar lijkt, zal dit worden gemeld bij de Dienst Recherche van het KLPD. Als het materiaal niet afkomstig is uit Nederland, zal melding worden gedaan bij partners in het netwerk van INHOPE, of zal de KLPD contact opnemen met buitenlandse opsporingsdiensten. Het meldpunt houdt zich alleen bezig met openbare

[75] http://www.meldpunt-kinderporno.nl.

verspreiding van kinderporno op het internet. Distributie via een-op-een e-mail bijvoorbeeld, valt buiten deze reikwijdte.

II. Toepassing bestaande regelgeving

Mede uit de interviews blijkt dat er een algemene bereidheid is bij internetserviceproviders om aan de bestrijding van distributie van kinderporno bij te dragen. Internetserviceproviders zijn bereid gevolg te geven aan meldingen door de bevoegde autoriteiten en private partijen, zoals het Meldpunt Kinderporno op Internet. Het meldpunt speelt een actieve rol in de evaluatie van de meldingen en het informeren van de bevoegde autoriteiten.

III. Ontwikkelingen

Het Meldpunt Kinderporno op Internet heeft gepleit voor plannen om kinderpornografisch materiaal te filteren. Momenteel wordt dergelijke filtering ontwikkeld en is er onder meer een pilot waarbij gebruik wordt gemaakt van hash-filtering-technologie, zoals ontwikkeld door de internetprovider Leaseweb.[76]

Het Platform Internetveiligheid, een initiatief van Nederlandse overheidsinstanties en particuliere bedrijven, dat wordt gecoördineerd door het Platform voor de InformatieSamenleving (ECP-EPN), heeft de ontwikkeling aangekondigd van een zwarte lijst ter bestrijding van verspreiding van kinderpornografie via het internet. De lijst zou moeten worden gehandhaafd door marktpartijen in afstemming met de overheid. Er zijn nog geen details verstrekt over de opmaak van deze lijst.[77] Het gebruik van een zwarte lijst voor het filteren van kinderporno heeft eerder plaats gevonden maar is weer afgeschaft. De betreffende zwarte lijst, die door het KLPD werd opgesteld, bleek niet gebaseerd te zijn op een adequate juridische grond.[78] De Nederlandse regering merkte in het verleden op dat filtering, als een middel ter bestrijding van illegale inhoud op het internet, tot op zekere hoogte ineffectief blijkt te zijn en het risico kent van uitbreiding naar andere informatie die niet illegaal is.[79]

Het Meldpunt Kinderporno op Internet heeft gepleit voor een multi-stakeholder-benadering, vergelijkbaar met de 'best practices van de Financial Coalition Against Child Pornography (FCACP), te vinden in de Internet Merchant Acquisition Best Practices for

[76] Meldpunt Kinderporno, 'Brief voor Algemeen overleg Tweede Kamer. Meldpunt Kinderporno op Internet, September 2009', http://www.meldpunt-kinderporno.nl/files/Biblio/Brief AO Kinderporno September 2009.pdf.
[77] http://www.ecp.nl/platform-internetveiligheid
[78] *Id.* p. 122-124.
[79] *Kamerstukken II* 2007-08, 28684, nr. 133, p. 14 en 22.

the Prevention and Detection of Commercial Child Pornography.[80] Deze coalitie wordt ook genoemd in de toelichting bij de wet tot omzetting van het Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik. Volgens de regering kan de samenwerking met banken en creditcard bedrijven van belang zijn voor het opsporen van verdachten, aangezien deze bedrijven functioneren als knelpunten die de financiële transactie faciliteren. Opgemerkt wordt dat deze bedrijven, verbonden door de FCACP, erkennen dat ze een zekere verantwoordelijkheid hebben in deze context.[81]

[80] http://www.fdic.gov/news/news/financial/2007/fil07072.html.
[81] *Kamerstukken II* 2009-10, 31810, nr. 3, p. 4-5.

Auteursrecht

I. Bestaande regelgeving

Wettelijk kader

Het auteursrecht is geregeld in de Auteurswet (AW). De wet beschermt rechthebbenden onder meer tegen ongeoorloofd gebruik, dat wil zeggen tegen ongeautoriseerde openbaarmaking en/of verveelvoudiging van auteursrechtelijk beschermde werken. Het downloaden van muziek of films is echter volgens de wet zonder voorafgaande toestemming van de rechthebbende toegestaan als een van de beperkingen van het auteursrecht van toepassing is. De meest relevante beperking in het kader van deze studie is de in artikel 16b en artikel 16c Aw geregelde beperking voor eigen gebruik (ook de thuiskopie genoemd). Voor de consument betekent een en ander dat hij content ook zonder toestemming van de rechthebbende mag downloaden.

Ook ten aanzien van de rol van internetserviceproviders in de context van auteursrechtelijke aspecten is het regime van artikel 6:196c van het *Burgerlijk Wetboek* (BW) van toepassing. Bij de totstandkoming is expliciet verwezen naar deze aspecten.[82]

Overige regulering

De Gedragscode Notice-and-Take-Down richt zich eveneens op klachten met betrekking tot auteursrechtelijke inbreuken.

II. Toepassing bestaande regelgeving

In de jurisprudentie zijn aanvullende randvoorwaarden/uitzonderingen geformuleerd met betrekking tot de toepassing van artikel 6:196c BW, voor zover het betreft de inbreuk op auteursrechten via de diensten van aanbieders die vallen onder het toepassingsgebied van dit artikel. In de zaak *BREIN/KPN Telecom BV* werd een website met bittorrents voor de distributie van door intellectuele eigendomsrechten beschermde werken als 'onmiskenbaar onrechtmatig' beschouwd. De verweerder KPN, in haar rol als aanbieder van toegang, werd door de voorzieningenrechter bevolen om de internetverbinding van de betreffende

[82] In de memorie van toelichting bij de wet Uitvoering richtlijn auteursrecht en naburige rechten in de informatiemaatschappij, wordt expliciet vastgesteld dat voor de aansprakelijkheid van tussenpersonen voor betrokkenheid bij online distributie van inbreukmakende informatie, de bepalingen over aansprakelijkheidsbeperkingen in de E-commerce richtlijn bepalend zijn: *Kamerstukken II* 2001-2002, 28482, nr 3, p. 38-39. Zie ook: *Kamerstukken II* 2005-2006, 30 392, nr. 6, p. 7.

abonnee af te sluiten als in de toekomst dezelfde onrechtmatige website op de faciliteiten van de provider zou worden geplaatst.[83] Er is in de literatuur betoogd dat een dergelijke verplichting ingaat tegen de limitatieve wijze waarop de voorwaarden van artikel 6:196c BW, in het bijzonder lid 1 met betrekking tot mere conduit activiteiten van internetserviceproviders, zijn geformuleerd. Het bevel is eveneens in het licht van de vrijheid van meningsuiting van de abonnee bekritiseerd.[84]

Andere recente rechtspraak betrof tussenpersonen die, volgens de rechter, buiten het toepassingsgebied vallen van de bepalingen zoals omschreven in artikel 6:196 c BW. In de zaken *BREIN/Mininova* en *BREIN/The Pirate Bay* worden de gedaagde partijen bevolen om te stoppen met het faciliteren van voortdurende schendingen van auteursrechten en/of andere intellectuele eigendomsrechten, dat wordt beschouwd als onrechtmatig onder algemeen aansprakelijkheidsrecht. Gezien hun betrokkenheid bij de inhoud die zij leveren, worden de eigenaars van deze websites geacht meer te verlenen dan activiteiten van 'diensten van de informatiemaatschappij', in de zin van artikel 6:196c BW. [85]

III. Ontwikkelingen

Onlangs heeft in Nederland op parlementair niveau de privé-exceptie in de huidige Auteurswet, op basis waarvan het kopiëren, en dus ook downloaden, van auteursrechtelijk beschermd materiaal voor privé doeleinden is vrijgesteld van auteursrechtelijke aanspraken door rechthebbenden, ter discussie gestaan. Bij deze discussie was tevens de vraag aan de orde of en op welke manier internetserviceproviders een rol kunnen spelen bij de handhaving van het voorgestelde nieuwe verbod op downloaden (van muziek en films) uit illegale bron. Er zijn voorstellen gedaan om hiervoor technieken te gebruiken, waarmee het internetverkeer structureel kan worden gecontroleerd op het niveau van doorgegeven bestanden, zoals ‘deep packet inspection’ en ‘finger printing’. Bovendien dient volgens de commissie wettelijk te worden geregeld dat Nederlandse internetserviceproviders of hostingproviders klantgegevens beschikbaar hebben van personen of bedrijven die via hun infrastructuur websites opzetten.[86] De Nederlandse regering heeft in een eerste reactie aangegeven het met de werkgroep eens te zijn dat er op verschillende terreinen van het auteursrecht problemen bestaan die moeten worden aangepakt.[87] De voorstellen van de commissie hebben op dit moment nog niet tot concrete wetsvoorstellen geleid.

---

[83] Rechtbank Den Haag (Vzr.) 5 januari 2007, *Auteurs-, Media- en Informatierecht* 2007-2 nr. 9 m.nt. O.L. van Daalen; *Computerrecht* 2007-2, 46 m.nt. L.A.R. Siemerink BREIN versus KPN Telecom.

[84] Chavannes (2007).

[85] Rechtbank Utrecht 26 augustus 2009, *LJN* BJ6008, BREIN versus Mininova; Rechtbank Amsterdam (Vzr.) 22 oktober 2009, *LJN* BK1067 The Pirate Bay versus BREIN.

[86] *Kamerstukken II* 2009-2010, 29838 en 31766, nr. 19 (herdruk), p. 34-35.

[87] *Kamerstukken II* 2009-2010, 29838, nr. 22.

Identiteitsfraude

I. Bestaande regelgeving

Wettelijk kader

Identiteitsfraude online is als zodanig niet strafbaar in Nederland.[88] Alleen de gevolgen van identiteitsfraude zijn strafbaar. Zo is creditcard fraude volgens artikel 232 van het *Wetboek van Strafrecht* (Sr) alleen strafbaar als de creditcard is gebruikt door de fraudeur om zichzelf of een ander te bevoordelen. De fraude als zodanig kan niet leiden tot een strafrechtelijke veroordeling. Artikel 11.7 lid 4 van de *Telecommunicatiewet* (Tw) vereist het gebruik van een ware identiteit in spamberichten. Het gebruik van een valse identiteit in dergelijke berichten kan van invloed zijn op de hoogte van de bestuurlijke boete die kan worden opgelegd in het kader van de Nederlandse Telecommunicatiewet.

Aangezien online identiteitsfraude op zichzelf niet strafbaar is onder het Nederlandse strafrecht, is het niet meteen evident welke maatregelen van internetserviceproviders, die vallen onder het toepassingsgebied van artikel 6:196c BW, gevergd kunnen worden wanneer ze te maken hebben met identiteitsfraude door middel van hun faciliteiten. Internetserviceproviders hebben geen algemene verplichting om toe te zien op de informatie die zij doorgeven of opslaan, of om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden. In verband met hosting van frauduleuze websites, betekent het feit dat de frauduleuze informatie op zichzelf niet strafbaar is en dus niet 'onmiskenbaar onrechtmatig', dat internetserviceproviders het materiaal niet hoeven te verwijderen om een succesvol beroep te kunnen doen op de uitsluiting van aansprakelijkheid waarin artikel 6:196c lid 4 BW voorziet.

Overige regulering

Ten aanzien van de Gedragscode Notice-and-Take-Down kan worden opgemerkt dat 'ongewenste inhoud' als een aparte categorie in de gedragscode wordt genoemd ten aanzien waarvan wordt voorgesteld dat tussenpersonen zelf kunnen beslissen welke soorten informatie eronder vallen en of ze daarmee op dezelfde wijze willen omgaan als met onrechtmatige en strafbare inhoud. Aangezien vormen daarvan niet als zodanig strafbaar zijn onder het Nederlandse strafrecht zou online identiteitsfraude kunnen worden opgevat als 'ongewenste inhoud'.

---

[88] Fraude met reisdocumenten is wel op zichzelf strafbaar. Zie artikel 231 Sr. Ook impliceert identiteitsfraude activiteiten die in strijd zijn met de Wbp.

De Nederlandse overheid heeft, op initiatief van het Ministerie van Binnenlandse Zaken en het Ministerie van Justitie, het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) opgezet. Dit meldpunt is een voortzetting van een proefproject dat in 2008 begon.[89] Deze proef was de voortzetting van een voormalig particulier initiatief, dat deel uitmaakte van vrijwillige initiatieven van de Stichting Aanpak Financieel-Economische Criminaliteit. [90]

II. Toepassing bestaande regelgeving

Overige regulering

Het CMI is officieel erkend door de betrokken Nederlandse ministeries als een definitieve dienst met ingang van 1 maart 2010. De activiteiten zijn in ontwikkeling.

III. Ontwikkelingen

Zie de ontwikkelingen die zijn geschetst bij het thema internetveiligheid, waaronder de plannen voor een bredere meldingsplicht inzake het verlies van persoonlijke gegevens als gevolg van een inbreuk op de beveiliging.

[89] See: http://www.overheid.nl/identiteitsfraude
[90] See: http://www.identiteitsfraude.nl/index.php?s=p_1&p=9

Verkoop gestolen goederen

I. Bestaande regelgeving

Wettelijk kader

Volgens artikel 417bis van het *Wetboek van Strafrecht* (Sr) is strafbaar hij die een goed verwerft, voorhanden heeft of overdraagt, dan wel een persoonlijk recht op of zakelijk recht ten aanzien van een goed vestigt of overdraagt, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van het goed dan wel het vestigen van het recht redelijkerwijs had moeten vermoeden dat het een door misdrijf verkregen goed betrof.

Voor zover relevant is artikel 6:196c BW onverkort van toepassing.

Overige regulering

De Gedragscode Notice-and-Take-Down speelt eveneens een rol bij de handel in gestolen goederen via het internet.

II. Toepassing bestaande regelgeving

Wettelijk kader

Bij de toepassing van de regulering – zo blijkt uit de praktijk – spelen internetserviceproviders geen rol, maar ligt het accent met name op de aanbieders van platforms.

In de zaak *Stokke/Marktplaats* rees de vraag of de website van Marktplaats, een Nederlandse dochteronderneming van eBay, de plicht heeft om de contactgegevens van gebruikers te verzamelen, in het bijzonder namen, adressen en woonplaatsen (NAW-gegevens). Alvorens deze vraag te beantwoorden, trok de rechtbank in een tussenvonnis de conclusie dat het een beslissing over eventuele plichten voor dit soort veilingsites onder het algemene recht inzake onrechtmatige daad, met name artikel 6:162 BW, niet achterwege hoefde te laten, indien een dergelijke website, als hosting provider, onder het regime van artikel 6:196c lid 4 BW valt, dat een lex specialis is ten opzichte van artikel 6:162 BW. De rechtbank liet vervolgens in het midden of Marktplaats nu wel of geen hostingdiensten verricht in de zin van artikel 6:196c lid 4 BW. Volgens de rechtbank waren er, gelet op de E-commerce

richtlijn en het doel en de parlementaire geschiedenis van artikel 6:196c lid 4 BW, mogelijkheden op grond van het algemene recht inzake onrechtmatige daad, maatregelen van Marktplaats te vergen om schade als gevolg van op intellectuele eigendomsrechten inbreukmakend materiaal te beperken of te voorkomen. De rechtbank concludeerde dat in dit geval een voorzorgsmaatregel in de vorm van preventieve monitoring van de advertenties op de website disproportioneel was in verhouding tot de betrokken belangen. De notice and take down procedure die Marktplaats ten uitvoer hanteerde voldeed aan de eisen van de zorg die men mag verwachten van Marktplaats.[91] Op het verzoek om van Marktplaats te verlangen dat zij NAW-gegevens van haar adverteerders registreerde, om deze beschikbaar te hebben voor afgifte wanneer een partij als Stokke in haar rechten zou zijn geschonden, oordeelde de rechtbank dat dit disproportioneel zou zijn. In deze context, merkte de rechtbank op dat het verwijzen van partijen, zoals Stokke, naar aanbieders van e-mailadressen, die Marktplaats wel van al haar gebruikers registreert, om zo NAW-gegevens te achterhalen, geen alternatief vormde omdat deze diensten te ver verwijderd zijn van de schadelijke inbreuk.[92]

Overige regulering

Platform aanbieders blijken veelal te beschikken over eigen procedures gericht op het tegengaan van de handel in gestolen goederen in een online-omgeving. Platforms als eBay en Marktplaats kennen een eigen notice and take down regime, dat mede is gebaseerd op het zogenaamde VeRO-programma (Verified Rights Owner).[93] Dit programma omvat richtlijnen over de wijze waarop op meldingen van inbreuken op intellectuele eigendomsrechten moet worden gereageerd.

[91] Rechtbank Zwolle/Lelystad, 3 mei 2006, *LJN* AW6288, Stokke A.S. versus Marktplaats B.V..
[92] Rechtbank Zwolle/Lelystad, 14 maart 2007, Stokke A.S. versus Marktplaats B.V. [zie overweging 2.5]. Vergelijk ook: Rechtbank Utrecht (Vzr.) 9 juli 2002, *LJN* AE5537 Teleatlas versus Planet Media Group.
[93] http://pages.ebay.nl/vero/

Verenigd Koninkrijk

Inleiding

I. Bestaande regelgeving

Wettelijk kader

De Electronic Commerce (EC Directive) Regulations 2002 implementeert de E-commerce richtlijn in het wetstelsel van Groot-Brittannië. Deze regeling schept het raamwerk ten aanzien van de aansprakelijkheid van internetserviceproviders. In lijn met de E-commerce richtlijn zijn deze tussenpersonen onder bepaalde voorwaarden uitgesloten van aansprakelijkheid voor inbreukmakend materiaal of inbreukmakende activiteiten.

Geheel in lijn met de richtlijn bepaalt artikel 17 dat dienstenaanbieders zijn uitgesloten van aansprakelijkheid indien zij zich slechts met mere conduit bezighouden. Deze bepaling is van toepassing in het geval een dienstenaanbieder van een ander afkomstige informatie doorgeeft of toegang tot een communicatienetwerk verschaft. Het artikel is derhalve van belang voor internetserviceproviders in hun hoedanigheid als aanbieders van internettoegang.

Artikel 18 regelt dat een dienstenaanbieder die zich bezighoudt met caching van materiaal niet aansprakelijk kan worden gesteld voor inbreuken indien deze geschieden via een geautomatiseerd werk en de tijdelijke opslag slechts in dienst staat van het bieden van een efficiëntere service. Deze uitzondering is slechts dan van toepassing wanneer de tussenpersoon de desbetreffende informatie niet wijzigt, de toegangsvoorwaarden voor de informatie in acht neemt, de regels met betrekking tot het bijwerken van de informatie opvolgt en de regels voor het verkrijgen van gegevens over het gebruik van de informatie niet wijzigt. Bovendien dient de dienstenaanbieder prompt de nodige maatregelen te treffen ter verwijdering van de informatie of om de toegang daartoe onmogelijk te maken, zodra hij weet dat de informatie is verwijderd van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe onmogelijk is gemaakt, of dat een rechter of een administratief orgaan zo heeft bevolen.

In artikel 19 is ten slotte bepaald dat een tussenpersoon die zich bezighoudt met hosting van materiaal onder bepaalde voorwaarden is uitgesloten van aansprakelijkheid. Deze bepaling is van toepassing wanneer de geleverde dienst bestaat uit de opslag van de door een afnemer van de dienst verstrekte informatie. De dienstenaanbieder is niet aansprakelijk of

strafbaar voor de op het verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat de tussenpersoon geen weet heeft van het onrechtmatige karakter van de activiteit of informatie en, in geval er een schadevergoedingsvordering is ingesteld, dit ook redelijkerwijs niet behoorde te weten. Zodra hij weet of redelijkerwijs behoort te weten dat op zijn netwerk zich onrechtmatig materiaal bevindt, verwijdert hij dit prompt of maakt de toegang daartoe onmogelijk. De laatste voorwaarde voor uitsluiting van aansprakelijkheid is dat de persoon die het materiaal heeft geplaatst niet onder de macht of invloed van de dienstenaanbieder mag staan.

In de regulering zijn niet alleen de bepalingen van de richtlijn overgenomen met betrekking tot mere conduit, hosting en caching. Artikel 22 geeft bovendien een nadere invulling aan de definitie van de 'notice', bij ontvangst waarvan de tussenpersoon wordt geacht kennis te hebben genomen van mogelijk onrechtmatige praktijken in verband met caching of hosting. Het artikel stelt dat de rechter in zijn oordeel alle omstandigheden van het geval moet laten meewegen en in zijn afweging betreffende de aansprakelijkheid van de dienstenaanbieder moet meenemen of de tussenpersoon een kennisgevingsbericht heeft ontvangen. In dit kennisgevingsbericht moet zijn vervat de naam en het adres van de verzender, gegevens omtrent de locatie van het desbetreffende materiaal en over het onrechtmatige karakter van de activiteit of het materiaal. Artikel 6(1)(c) bepaalt verder nog dat een tussenpersoon zijn contactgegevens, waaronder zijn e-mail adres, toegankelijk en openbaar moet maken om zulke kennisgeving mogelijk te maken. Op deze punten is de Britse implementatie van de E-commerce richtlijn uitgebreider dan de richtlijn zelf, aangezien die geen definitie geeft van 'notice', noch stelt welke informatie daarin moet zijn vervat.

Artikel 15 van de E-Commerce Richtlijn stelt dat Lidstaten geen algemene verplichting aan internetdienstenaanbieders mogen opleggen ten aanzien van het controleren van hun netwerk met betrekking tot de overdracht of opslag van materiaal of activiteiten. De Britse regering heeft expliciet afgezien van het implementeren van deze regel, mede om te voorkomen dat een dergelijke implementatie mogelijk weer strijdig zou kunnen zijn met de Richtlijn.

Internetveiligheid

I. Bestaande regelgeving

Wettelijk kader

De wettelijke inkadering van internetveiligheid is terug te vinden in de Privacy and Electronic Communications (EC Directive) Regulations 2003. Hiermee wordt de Europese richtlijn inzake privacy en elektronische communicatie vrijwel letterlijk geïmplementeerd. Artikel 5, dat een letterlijke implementatie van artikel 4 van de Richtlijn is, regelt de verantwoordelijkheden met betrekking tot beveiliging.

Overige regulering

Overige regulering bestaat primair uit zelfregulering door de betrokken marktpartijen. Daarbij gaat het onder meer om regulering inzake spam en malware. De belangenorganisatie van internetserviceproviders, ISPA-UK, kent naast een algemene code of conduct (waarop onder het volgende thema zal worden ingegaan) een drietal 'Current Best Practices' (CBP): a) BCP on Blocking and filtering of Internet traffic; b) BCP on Unsolicited Bulk Email (spam) en c) BCP on Law Enforcement Contact. [94] In de eerste wordt onder meer bepaald dat in het geval van filtering de gebruikers op juiste wijze moeten worden geïnformeerd. De tweede inzake spam draagt internetserviceproviders op ervoor te zorgen dat iedere e-mail die binnen hun eigen netwerk wordt gegenereerd aan een bepaalde gebruiker of aan een bepaald systeem kan worden gekoppeld. Bovendien moeten er afdoende maatregelen worden getroffen met betrekking tot het afhandelen van berichten betreffende misbruik van hun klanten. Als het misbruik wordt bewezen moet de tussenpersoon effectieve maatregelen treffen om dit misbruik een halt toe te roepen. De derde Current Best Practices gaat in op de verschillende maatregelen die een internetserviceprovider moet treffen om bereikbaar te zijn voor verzoeken van onder meer justitie. Specifieke zelfregulering met betrekking tot internetveiligheid is niet aanwezig.

[94] http://www.ispa.org.uk/home/page_364.html.

II. Toepassing bestaande regelgeving

Wettelijk kader

De implementatie van de Privacy and Electronic Communications (EC Directive) Regulations 2003 heeft niet geleid tot verdere regulering. Gebruikers worden op de website van de toezichthouder, de OFCM, doorverwezen naar hun internetserviceprovider.

Overige regulering

Zoals hierboven is vermeld, zijn er geen bindende maatregelen van kracht die met betrekking tot de integriteit en de veiligheid van informatie technologie systemen zorgplichten aan tussenpersonen opleggen. Wel is de Best Current Practice betreffende Unsolicited Bulk Email geïmplementeerd. Deze legt echter geen bindende verplichtingen op. Alhoewel deze maatregelen in sommige gevallen effectief zijn, is dit niet noodzakelijkerwijs in het algemeen ook zo, aangezien zij afdwingbaarheid en een gecentraliseerde benadering missen.

Kinderpornografie

I. Bestaande regelgeving

Wettelijk kader

De belangrijkste wetgeving in het Verenigd Koninkrijk met betrekking tot de regulering van de distributie, het maken en het bezit van kinderpornografisch materiaal is vinden in de Protection of Children Act 1978 (die niet van toepassing is in Schotland en Noord-Ierland) en in sectie 160 van de Criminal Justice Act 1988 (die in het gehele Koninkrijk van toepassing is). De eerste wet stelt dat het afnemen, de verhandeling, het vertonen en het publiceren van kinderpornografische foto's strafbaar is. De Sexual Offences Act 2003, sectie 45, die sectie 7(6) van de Protection of Children Act 1978 amendeert, definieert een kind als een persoon onder de achttien. De Protection of Children Act is door sectie 84 van de Criminal Justice and Public Order Act 1994, zo uitgebreid dat onder 'foto' ook een foto in een elektronisch data format valt. De Criminal Justice Act maakt het enkele bezit van een aanstootgevende foto van een kind strafbaar.

Verder geeft – zoals beschreven in de inleiding – de implementatie van de E-commerce richtlijn het raamwerk voor de verantwoordelijkheden van dienstenaanbieders op het internet voor onrechtmatig materiaal en activiteiten op hun netwerk en derhalve ook voor kinderpornografisch materiaal. In de interviews kwam naar voren dat aanbieders ruime verantwoordelijkheden onderkennen met betrekking tot kinderporno, maar tegelijkertijd geven zij aan dat deze mate van verantwoordelijkheid zich niet kan uitstrekken tot andere domeinen, zoals het auteursrecht.

Overige regulering

In aanvulling op de wettelijke maatregelen en in het licht van E-commerce richtlijn is een aantal andere maatregelen genomen om online kinderpornografisch materiaal te reguleren. Met betrekking tot de aansprakelijkheid van tussenpersonen op het internet is in 1996 de non-gouvernementele organisatie Internet Watch Foundation (IWF) opgericht, met als doel de wereldwijde bestrijding van met name kinderpornografisch materiaal op het internet (en in het Verenigd Koningrijk tevens van obsceen materiaal en materiaal waaruit rassenhaat blijkt). De IWF werkt samen met onder meer de online industrie, handhavingsinstanties, de overheid, de onderwijssector, en internationale partners om zo de beschikbaarheid van kinderpornografisch materiaal tegen te gaan.

De IWF voorziet ook in een notice and take down procedure. Zowel internetgebruikers als betrokken ondernemingen, waaronder internetserviceproviders, kunnen melding doen van obsceen materiaal bij de hotline van de organisatie. Dat kan via e-mail, telefoon of fax.

De organisatie wordt bestuurd door een Board of Trustees. Deze bestond oorspronkelijk uitsluitend uit vertegenwoordigers van tussenpersonen op het internet. Het huidige bestuur daarentegen bestaat uit een breed scala aan experts van verschillende organisaties en met verschillende achtergronden, waarmee een breed draagvlak is gecreëerd.

II. Toepassing bestaande regelgeving

Wettelijk kader

Het knelpunt van het bestaande wettelijke kader betreffende de distributie, de creatie en het bezit van kinderporno is de toepassing en handhaving in online situaties. Vaak staat voor de rechter de vraag ter discussie of bestaande wetgeving ook kan worden toegepast op de internetomgeving en haar opslagcapaciteiten en haar publicitaire en distributieve mogelijkheden. Zo is er onder meer geprocedeerd over de vraag of foto's die gecached waren bij een provider tot het bezit van een gebruiker konden worden gerekend.

Verder is in de interviews opgemerkt – hetgeen ook voor de andere onderzochte landen relevant is – dat de werking van de E-commerce richtlijn c.q. een notice and take down procedure zich primair beperkt tot materiaal dat zich in het publieke domain bevindt en dat derhalve door derden te detecteren is. Deze kunnen de dienstenaanbieder hierover vervolgens inlichten. Echter, het meeste kinderpornografische materiaal wordt verspreid via afgeschermde kanalen, zoals peer-2-peer netwerken en afgesloten nieuwsgroepen.

Overige regulering

Rond de 85 procent van de meldingen die de IWF ontvangt betreft kinderpornografisch materiaal (Child sexual abuse content), 10 procent betreft overig obsceen materiaal (criminally obscene adult content) en 5 procent betreft materiaal waaruit rassenhaat blijkt (incitement to racial hatred content). In 2008 heeft de organisatie 33947 klachten verwerkt.[95] De meeste meldingen betroffen materiaal dat buiten het Verenigd Koninkrijk werd gehost.

Bij ontvangst van een melding controleert de IWF het aangegeven materiaal op wederrechtelijkheid ten aanzien van de Britse wetgeving en wordt actie ondernomen indien strijdigheid daarmee wordt vastgesteld. De hiervoor verantwoordelijke werknemers zijn getraind door de Britse politie om hun taak adequaat te kunnen vervullen.

[95] http://www.iwf.org.uk/documents/20091214_iwf_annual_report_2008_pdf_version.pdf

Waarschijnlijk is de belangrijkste uitkomst van de inspanningen van de Internet Watch Foundation de dagelijks bijgehouden zwarte lijst van URL's waarop kinderpornografisch materiaal te vinden is. Deze lijst wordt doorgegeven aan Britse dienstenaanbieders op het internet, zodat zij het materiaal kunnen verwijderen of blokkeren. Thans blokkeert 98 procent van de Britse tussenpersonen materiaal op basis van deze zwarte lijst. Deze lijst wordt in gecodeerde vorm naar de tussenpersonen toegestuurd om illegaal gebruik te voorkomen, maar de tussenpersonen kunnen de lijst wel wijzigen en hun eigen URL's aan de lijst toevoegen. Daarnaast wordt de lijst toegezonden aan de Britse politie in het geval het desbetreffende materiaal uit het Verenigd Koningrijk afkomstig is. Als het materiaal afkomstig is uit het buitenland wordt door de IWF aan Britse internetserviceproviders verzocht om toegang te blokkeren. De melding wordt doorgegeven aan de zusterorganisatie in het desbetreffende land (voor zover aanwezig). Als er geen zusterorganisatie bestaat wordt de verantwoordelijke buitenlandse dienstaanbieder (in de regel een hostingorganisatie) geïnformeerd. Bovendien wordt de Serious Organised Crime Agency (SOCA) geïnformeerd, die contact opneemt met de buitenlandse politie om verwijdering van het materiaal te bewerkstelligen. Wanneer de IWF-blokkade wordt toegepast, zal er een 404 'technische fout' op de pagina verschijnen indien een browser toegang probeert te krijgen tot de pagina.

Verder kent de organisatie van internetserviceproviders ISPA UK een Code of Practice.[96] Deze code specificeert een aantal minimum standaarden met betrekking tot het tegengaan van illegaal materiaal op het internet. Alle leden van de organisatie dienen zich aan deze code houden. De code bevat in artikel 5 een verwijzing naar de werkzaamheden van de IWF. Alhoewel het lidmaatschap ISPA-UK als zodanig niet verplicht tot het lidmaatschap van de IWF moeten de leden zich wel houden aan de notice and take down procedure van die organisatie en verzoeken tot verwijdering uitvoeren.

De werkwijze van de IWF met een goedlopende hotline en een goedwerkend systeem waarbij URL's op een zwarte lijst worden geplaatst wordt over het algemeen als positief ervaren. Het wordt gezien als een snelle en praktische methode voor het verwijderen van kinderpornografisch materiaal. Bovendien ontlast de hotline van de Internet Watch Foundation onder meer de internetserviceproviders voor wat betreft het afhandelen van klachten.

III. Ontwikkelingen

Een aspect dat nog in de interviews werd genoemd betreft de opvoeding van de internetgebruiker in het algemeen en van de ouders in het bijzonder over het potentiële gevaar dat gepaard gaat met het gebruik van internet. In dit verband is het rapport 'Safer

Children in a Digital World: the Byron Review' uitgebracht waarin onder meer wordt gesteld dat, alhoewel het internet zeer populair is bij kinderen, er een gebrek is aan kennis en bewustzijn bij de ouders betreffende hun rol om zorg te dragen voor de veiligheid van hun kinderen op het internet met betrekking tot schadelijk materiaal.[97]

[96] http://www.ispa.org.uk/about_us/page_16.html
[97] http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

Auteursrecht

I. Bestaande regelgeving

Wettelijk kader

De belangrijkste wetgeving betreffende het gebruik, het kopiëren en de distributie van auteursrechtelijk beschermt materiaal in het Verenigd Koninkrijk is de Copyright, Designs and Patents Act 1988.[98] De wet geeft scheppers van een literair, dramaturgisch, muzikaal of artistiek werk het recht op controle betreffende de manier waarop hun werk wordt gebruikt. Bovendien geeft de wet verschillende rechtsmiddelen aan auteursrechthebbenden om zich tegen het ongeautoriseerd kopiëren van het werk te verzetten. Volgens artikel 17 van de wet valt onder 'inbreuk' het reproduceren van een werk in iedere materiële vorm, inclusief de opslag van materiaal door elektronische middelen. Sectie 18 van de wet bepaalt meer in het bijzonder dat het uitgeven van kopieën van een werk de auteursrechten van de rechthebbende schendt. Bovendien bepaalt artikel 107(1) dat het tevens strafbaar is om een inbreukmakende kopie van een auteursrechtelijk werk in het kader van de bedrijfsvoering te bezitten zonder een licentie daartoe van de auteursrechthebbende te hebben. Subparagraaf (e) bepaalt dat het strafbaar is om een inbreukmakende kopie te verspreiden anders dan in het kader van de bedrijfsvoering in zoverre dit de auteursrechthebbende schaadt.

Ook ten aanzien van de verantwoordelijkheden van internetserviceproviders op het gebied van het auteursrecht is de eerder beschreven implementatie van de E-commerce richtlijn leidend.

Overige regulering

In het Verenigd Koninkrijk bestaat geen zelfregulering met betrekking tot de rol van internetserviceproviders in relatie tot auteursrechtelijke inbreuken. Er is geen code of conduct of een voorgeschreven notice and take down procedure.

[98] http://www.opsi.gov.uk/acts/acts1988/UKpga_19880048_en_1.htm.

II. Toepassing bestaande regelgeving

Wettelijk kader

De Copyright, Designs and Patents Act geeft ook het raamwerk voor de aansprakelijkheid van tussenpersonen op het internet voor auteursrechtschendingen op hun netwerk. De vraag is of het transport van inbreukmakend materiaal door een dienstenaanbieder op het internet moet worden gezien als primaire of als secundaire inbreuk. Er bestaat geen specifieke jurisprudentie omtrent deze vraag. Echter in Sony Music Entertainment v Easyinternetcafe[99] heeft de rechter bepaald dat, alhoewel de aansprakelijkheid voor primaire auteursrechtschendingen onder de artikelen 17 en 18 strikt is (waarbij de afwezigheid van kennis van de inbreuk geen geldige verdedigingsgrond is), dit niet betekent dat dit regime zich uitstrekt over partijen, zoals tussenpersonen op het internet, die geen controlemogelijkheden hebben ten aanzien van de desbetreffende handelingen.

Overige regulering

In de interviews is naar voren gebracht dat de bestaande regulering als afdoende wordt ervaren. Internetserviceproviders hebben een eigen beleid met betrekking tot verzoeken om inbreukmakend materiaal te verwijderen. Daarnaast wordt er op gewezen dat rechtenhouders via een rechterlijk bevel verwijdering kunnen bewerkstelligen. Tenslotte is verwezen naar de ten tijde van de interviews nog in behandeling zijnde Digital Economy Act (zie hierna).

III. Ontwikkelingen

Op 8 april 2010 is de Digital Economy Act aangenomen.[100] In het kader van deze studie is relevant dat de wet een 'Graduated Response Procedure' introduceert. Een dergelijke procedure houdt kort gezegd in dat ten aanzien van een internet gebruiker die meermaals wordt betrapt op het schenden van auteursrechten van anderen, de Internetserviceprovider in het uiterste geval kan worden gevraagd deze persoon van het internet af te sluiten. De wet voegt artikelen 124A tot en met 124N in de Communications Act in en secties 17 en 18 van de Digital Economy Act geven de Secretary of State een aantal bevoegdheden. In artikelen 124A en 124B staan de zogenoemde Initial Obligations vermeld. Volgens artikel

[99] Sony Music Entertainment (UK) LtD & Others v Easyinternetcafe Ltd [2003] EWHC 62(Ch).

[100] http://www.opsi.gov.uk/acts/acts2010/pdf/ukpga_20100024_en.pdf; Memorie van toelichting: http://www.publications.parliament.uk/pa/ld200910/ ldbills/001/2010001. Zie ook de eerdere consultatie pdf http://www.berr.gov.uk/consultations/page51696.html.

124A kan een auteursrechthebbende een Internetserviceprovider een kennisgevingsbericht van een inbreuk op zijn auteursrecht sturen. Dit kennisgevingsbericht moet de inbreuk zelf vermelden, een beschrijving geven van de inbreuk, het IP adres van de internetgebruiker bevatten en het moment vermelden waarop het bewijs is verzameld. Het kennisgevingsbericht moet naar de Internet Acces Provider worden gestuurd binnen een periode van één maand beginnend op de dag waarop de informatie is verzameld. Artikel 124B bevat de tweede Initial Obligation, namelijk de verplichting van de Internet Access Provider om per internetgebruiker een lijst met kennisgevingsberichten bij te houden. Deze lijst mag ook de kennisgevingsberichten van andere auteursrechthebbenden bevatten, zodat de auteursrechthebbende kan bepalen of de desbetreffende persoon bij gewoonte inbreuk maakt of niet. Men hoopt dat auteursrechthebbenden zodoende alleen diegenen in rechte zullen aanspreken die op grote schaal inbreuk maken en dat zij de eenmalige overtreders met rust zullen laten. Hierdoor worden de rechtsmiddelen op effectieve en efficiënte ingezet. Een auteursrechthebbende die een provider heeft ingelicht over een inbreuk mag de lijst met bewaarde gegevens opvragen bij de Internet Acces Provider. Deze lijst mag niet de identiteit van de internetgebruiker openbaren.[101] Om achter de identiteit te komen zal de auteursrechthebbende een rechterlijk bevel moeten vragen. Nadat hem de identiteit van de desbetreffende persoon is geopenbaard kan de auteursrechthebbende hem voor schadevergoeding aanspreken.

De Initial Obligations worden slechts dan van kracht indien er een zogenoemde Initial Obligations Code is vervaardigd. Deze Code moet volgens artikelen 124C tot 124E voorzien in procedurele criteria, zoals het format, de vereiste informatie en de tijdsrestricties met betrekking tot zowel het door de auteursrechthebbende aan de provider verzonden rapport als het door de provider aan de internetgebruiker verzonden kennisgevingsbericht daarvan, en de lijst met belastende informatie die door de provider per gebruiker wordt bijgehouden. De Code mag ook vrijwillige bepalingen bevatten, indien de partijen daarover overeenstemming bereiken. Men hoopt dat alle belanghebbenden, waaronder de auteursrechthebbenden, de dienstenaanbieders op het internet en hun klanten, zullen bijdragen aan de totstandkoming van deze Code.[102] Artikel 124C bepaalt dat de regulerende autoriteit, de Office of Communications, akkoord moet gaan met een dergelijke Code en artikel 124D bepaalt dat als zij dat niet doet of als er geen Code tot stand is gekomen, de Office of Communications er dan zelf één zal vervaardigen.

De Secretary of State mag technische verplichtingen opleggen aan internetserviceproviders, op grond waarvan zij verplicht zijn om maatregelen te nemen tegen hun gebruikers in de zin van een beperking op de snelheid of capaciteiten van de geleverde dienst, een beperking of een limiet op de toegang tot bepaald materiaal of, in het uiterste geval, het afsluiten van de toegang tot het internet.[103] Om beter te kunnen bepalen welke maatregelen aan welke

[101] Digital Economy Bill, Explanatory notes, p. 9. http://www.publications.parliament.uk/pa/ld200910/ldbills/001/2010001. Zie ook de eerdere consultatie pdf http://www.berr.gov.uk/consultations/page51696.html

[102] Digital Economy Bill. Explanatory notes, p. 10.

[103] See also: http://www.berr.gov.uk/consultations/page51696.html

provider moeten worden opgelegd, maakt OFCOM rapporten ter beoordeling van de situatie. De Secretary of State mag op basis daarvan, of daaraan voorbijgaande, een provider verplichten om technische maatregelen te nemen tegen zijn gebruikers in het geval zij aan bepaalde, vastgelegde criteria voldoen.[104] OFCOM moet daarop een Technical Obligations Code maken waarin de verplichtingen en de maatregelen worden gespecificeerd. Hierin wordt ook een procedure opgenomen om klachten van de klant af te handelen. In deze code wordt ook bepaald wat de gronden voor deze klachten mogen zijn en wat moet worden meegewogen in de vaststelling van de schuld van de gebruiker.

Zowel de Initial Obligations Code als de Technical Obligations Code bepalen dat er een, in relatie tot de providers, de auteursrechthebbenden en de Office of Communications, neutraal persoon moet worden aangewezen om klachten van internetgebruikers te behandelen. Deze klachten kunnen verband houden met de vermeende inbreuk of met de identificatie van de gebruiker als degene die de inbreuk heeft gemaakt. Ook mogen de klachten zich richten tegen het door de provider in een lijst bewaren van informatie over de gebruiker.

Artikel 124K bepaalt dat er ook beroep tegen de technische verplichtingen openstaat bij een zogenaamd First-tier Tribunal. Dit is een algemene rechterlijke instantie voor beroep tegen overheidsbeslissingen, die de macht heeft om beslissingen terug te draaien, terug te verwijzen of beslissingen te bevestigen. Ook kunnen kostenvergoedingen worden toegewezen. Eventuele technische maatregelen zullen waarschijnlijk worden opgeschort tot na de rechterlijke uitspraak.[105]

Artikel 124L bepaalt dat de internetserviceprovider die niet meewerkt aan de voorbeschreven procedure, kan worden beboet met een bedrag van maximaal £250.000.

[104] Digital Economy Bill. Explanatory notes, p. 12.
[105] Digital Economy Bill. Explanatory notes, p. 12.

Identiteitsfraude

I. Bestaande regelgeving

Wettelijk kader

Er bestaat in het Verenigd Koninkrijk geen wetgeving die expliciet ingaat op identiteitsfraude. Wel is in 2006 de Fraud Act uitgevaardigd, die ook kan worden toegepast in het geval van identiteitsfraude. Onder deze wet is noch enig bewijs van misleiding noch het verkrijgen van enig gewin vereist. Artikel 1 van de wet creëert een nieuw algemeen fraude artikel, waarin is bepaald dat fraude kan worden begaan op drie manieren: door een valse voorstelling van zaken (artikel 2); door het niet openbaren van informatie (artikel 3); en door misbruik van positie (artikel 4). Artikel 2 stelt meer in het bijzonder dat de persoon in strijd handelt met die bepaling indien hij: (a) te kwader trouw een valse voorstelling van zaken geeft, (b) met als doel (i) om profijt voor hemzelf of een ander te verkrijgen, of (ii) om een ander schade te berokkenen of een ander aan een bepaald gevaar bloot te stellen.

Er bestaat echter geen geformaliseerde zorgplicht voor tussenpersonen op het internet met betrekking tot identiteitsfraude.

II. Toepassing bestaande regelgeving

Wettelijk kader

De Fraud Act wet is gezien de ruime strekking onder meer van toepassing op iedere vorm van phishing activiteit, inclusief het zenden van spoof e-mails naar niets vermoedende bedrijven en individuen (fishing) en het zenden van gerichte phishing e-mails (spear phishing).[106]

Voorlichting over identiteitsfraude is bijvoorbeeld onderdeel van een door de overheid en het bedrijfsleven opgezette publiekscampagne.[107] Er wordt geen bijzondere aandacht geschonken aan de rol van internetserviceproviders, het accent ligt meer bij de partijen die te maken krijgen met de gevolgen van identiteitsfraude.

[106] A Savirimuthu, J Savirimuthu, "Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective", (2007) 4:4 SCRIPTed 436.
[107] http://www.identitytheft.org.uk/

Verkoop gestolen goederen

I. Bestaande regelgeving

Wettelijk kader

Handel in gestolen goederen is in het Verenigd Koninkrijk gereguleerd bij de Theft Act 1968. Volgens artikel 22 is er sprake van een overtreding indien een persoon handelt in gestolen goederen als (anders dan bij stelen) hij bij de verkrijging ervan weet of denkt dat het gestolen goederen betreft of als hij te kwader trouw actie onderneemt of assisteert bij het behoud, de verwijdering, de vernietiging van de goederen of de goederen te gelde maakt voor het gewin van een andere persoon, of als hij daartoe opdracht geeft. Binnen de reikwijdte van dit artikel valt ook het zogenoemde 'e-fencing', dat refereert naar de online verkoop van gestolen goederen.

De bepalingen in het kader van de implementatie van de E-commerce richtlijn brengen met zich mee dat internetserviceproviders erop attent kunnen worden gemaakt dat er gestolen goederen worden verhandeld via hun netwerk/diensten en dat hen kan worden gevraagd gepaste maatregelen te nemen.

Overige regulering

Er bestaat geen andere regulering met betrekking tot zorgplichten van tussenpersonen op het internet om de handel in gestolen goederen tegen te gaan. Wel is bekend dat de belangrijkste marktpartij, eBay, eigen procedures kent ter voorkoming van de handel in gestolen goederen.

II. Toepassing bestaande regelgeving

Wettelijk kader

Zoals aangegeven valt 'eFencing', de online verkoop van gestolen goederen, onder artikel 22 Theft Act. Hierbij moet een onderscheid worden gemaakt tussen de handel in goederen die al eerder gestolen zijn en de handel in goederen waarmee het intellectueel eigendomsrecht van een ander wordt geschonden. Met betrekking tot de laatste handeling bestaat er jurisprudentie ten aanzien van hosting van materiaal door tussenpersonen op het internet (i.e. online veilinghuizen).

Recente jurisprudentie heeft uitgewezen dat het Verenigd Koninkrijk terughoudend is met betrekking tot het toedichten van verantwoordelijkheden aan intermediairs, in dit geval van online veilinghuizen, voor materiaal dat door gebruikers wordt aangeboden. In L'Oréal v. eBay heeft de High Court van het Verenigd Koninkrijk in het voordeel van eBay geoordeeld en de organisatie vrijgesproken van aansprakelijkheid voor door gebruikers aangeboden materiaal dat inbreuk maakt op het merkrecht van anderen. Er zijn in deze zaak prejudiciële vragen gesteld aan het Europese Hof.[108]

Overige regulering

Online veilinghuizen, in het bijzonder Ebay, hebben eigen maatregelen getroffen om de handel in gestolen goederen tegen te gaan. Ebay heeft strikte interne regels en voert een eigen beleid betreffende de handel in gestolen goederen en werkt op dit punt nauw samen met justitie inzake vervolging (zie ook de Nederlandse landenstudie).

[108] http://www.judiciary.gov.uk/docs/judgments_guidance/l'oreal-ebay.pdf. Prejudiciële vragen: Publ C 267/40 d.d. 7/11/2009, zaak C-324/09)

Duitsland

Inleiding

I. Bestaande regelgeving

Wettelijk kader

De bepalingen van de E-commercerichtlijn zijn terug te vinden in de artikelen 7 tot en met 10 van het Duitse *Telemediengesetz* (TMG). Volgens artikel 8 TMG heeft een internetserviceprovider een verminderde aansprakelijkheid als hij informatie doorgeeft in een communicatienetwerk of toegang verschaft tot informatie van derden. Dit is het geval wanneer de dienstenaanbieder de doorgifte niet heeft geïnitieerd, niet de ontvanger van informatie heeft gekozen en de informatie niet heeft geselecteerd of gewijzigd. De aansprakelijkheidsvermindering geldt ook als de data tijdelijk wordt opgeslagen ten behoeve van de doorgifte in een communicatienetwerk zolang de data niet langer dan nodig wordt opgeslagen.

De artikelen 9 en 10 TMG zijn relevant voor tussenpersonen die informatie van derden cachen of hosten. Artikel 9 TMG bepaalt dat een dienstenaanbieder is gevrijwaard van aansprakelijkheid als hij automatisch en tijdelijk informatie van derden opslaat met het oog op de doorgifte aan anderen en hij (1) de informatie niet wijzigt, (2) de toegangsvoorwaarden voor de informatie in acht neemt, (3) de alom erkende en in de bedrijfstak gangbare regels betreffende het bijwerken van de informatie naleeft, (4) en de rechtmatige verkrijging van gegevens over het gebruik van de informatie niet hindert. De tussenpersoon dient bovendien prompt de informatie te verwijderen of de toegang ertoe onmogelijk te maken zodra hij daadwerkelijke kennis heeft van het feit dat de informatie van de oorspronkelijke bron is verwijderd of de toegang ertoe onmogelijk is gemaakt, of op een daartoe strekkende vordering.

Artikel 10 TMG bepaalt dat een tussenpersoon van aansprakelijkheid is gevrijwaard wanneer hij (1) informatie opslaat voor een gebruiker zonder dat hij daadwerkelijke kennis van de onrechtmatige informatie heeft en, als het schadevergoedingsvordering betreft, hij geen kennis heeft van feiten of omstandigheden waaruit het onrechtmatige karakter van de activiteiten of informatie duidelijk blijkt. Verder (2) dient de tussenpersoon, wanneer hij kennis heeft genomen van de onrechtmatigheid van de informatie, de informatie onmiddellijk te verwijderen of de toegang ertoe onmogelijk maken. Deze vrijwaring geldt alleen als de persoon die de informatie online plaatst niet op gezag of onder toezicht van de tussenpersoon handelt.

In lijn met de E-commerce richtlijn bevat de TMG geen wettelijke notice and take down-procedure. Ook is in artikel 7 TMG expliciet opgenomen dat tussenpersonen geen algemene verplichting hebben om de informatie die zij doorgeven te onderzoeken op onrechtmatige activiteiten. Tussenpersonen zijn dus slechts verplicht om op te treden wanneer zij door derden van onrechtmatige activiteiten op de hoogte worden gesteld. Artikel 7 TMG regelt overigens ook dat het (tele)communicatiegeheim, zoals dat wordt beschermd in artikel 88 van het Duitse *Telekommunikationsgesetz* (TKG), gewaarborgd moet worden bij elk van de hierboven beschreven activiteiten. Deze bescherming reikt verder dan de E-commerce richtlijn voorschrijft, maar is verplicht op basis van het Duitse dataprotectierecht. Artikel 88 TKG stelt dat iedere tussenpersoon verplicht is om het (tele)communicatiegeheim te beschermen, ook nadat de tussenpersoon zijn activiteiten heeft gestaakt. Verder is bepaald dat bijkomende aspecten van het communicatieproces ook door het (tele)communicatiegeheim worden beschermd. Het (tele)communicatiegeheim is ook van toepassing op mislukte communicatiepogingen.

Internetveiligheid

I. Bestaande regelgeving

Wettelijk kader

De zorgplicht en aansprakelijkheid van tussenpersonen voor de veiligheid en integriteit van netwerken en computersystemen van gebruikers is afhankelijk van waar de veiligheidsinbreuk plaatsvindt. In het algemeen kan men twee scenario's onderscheiden: (a) de veiligheid en integriteit van systemen van de tussenpersoon en (b) de veiligheid en integriteit van systemen van de eindgebruiker.

Artikel 7 lid 1 TMG bepaalt dat de verminderde aansprakelijkheid van tussenpersonen, zoals die gedefinieerd is in artikelen 8 tot en met 10 TMG, niet van toepassing is op eigen informatie, dus ook niet op de veiligheid van eigen systemen. De verminderde aansprakelijkheid is slechts van toepassing op informatie, maar niet het functioneren of de veiligheid van de diensten die door de tussenpersonen worden aangeboden. Twee scenario's dienen daarom te worden onderscheiden. Als de integriteit en veiligheid van de data van een gebruiker is geschonden door een inbreuk in en manipulatie van het systeem van de tussenpersoon, dan geldt de vermindering van aansprakelijkheid niet. Wanneer daarentegen de integriteit en de veiligheid van het systeem van de gebruiker wordt geschonden (doordat de internetserviceprovider kwaadaardige data heeft doorgegeven, dan wel doordat een derde, die ook een gebruiker is, kwaadaardige data heeft opgeslagen op de server van een hosting provider), dan is de verminderde aansprakelijkheid, zoals geregeld in artikelen 8 tot en met 10 TMG, wel van toepassing.

Tussenpersonen hebben dus een zorgplicht om hun systemen in voldoende mate te beschermen tegen veiligheidsinbreuken en het schenden van de integriteit en veiligheid van gebruikersdata (zoals de vernietiging of het verlies van data en de vernietiging van hardware als gevolg van schadelijke software). Als een tussenpersoon niet aan zijn zorgplicht voldoet en schade wordt toegebracht aan de gebruikerszijde, dan kan de gebruiker van de tussenpersoon een schadevergoeding eisen. Uit de zorgplicht kan bijvoorbeeld het gebruik van virusscanners en firewalls volgen.

Opgemerkt moet echter worden dat ten aanzien van schadevergoedingsclaims tegen telecommunicatiediensten geldt dat artikel 44a TKG de geldelijke aansprakelijkheid van deze dienstenaanbieders limiteert tot 12.500 euro.

In het geval dat de inbreuk op de integriteit en de veiligheid plaatsvindt bij het systeem van de gebruiker, of dat deze wordt veroorzaakt door een derde partij, dan zijn de aansprakelijkheidsverminderingen van artikelen 7 tot en met 10 TMG van toepassing. Dit betekent dat tussenpersonen geen zorgplicht hebben voor data die zij overbrengen, hosten

of cachen en voor data die de integriteit en veiligheid van de systemen van hun gebruikers schendt, tenzij zij hiervan op de hoogte worden gesteld of daarvan kennis nemen. Van dit laatste kan echter al sprake zijn wanneer door een tussenpersoon ongebruikelijk netwerkverkeer of ongebruikelijke netwerkactiviteiten worden vastgesteld. Er rust evenwel geen plicht op tussenpersonen om netwerkverkeer te onderzoeken op zulke ongebruikelijkheden, zoals ook in de inleiding is aangegeven.

Artikel 4 van de richtlijn Privacy en elektronische communicatie voegt daaraan toe dat de aanbieder van een openbare telecommunicatiedienst passende technische en organisatorische maatregelen moet treffen om de veiligheid van de aangeboden diensten te garanderen. Deze bepaling is naar Duits recht omgezet in artikel 109 TGK, waarin is bepaald dat dienstenaanbieders passende technische of andersoortige maatregelen moeten treffen om het (tele)communicatiegeheim te waarborgen en om telecommunicatie en andere dataverwerkingssystemen te beschermen tegen ongeautoriseerde toegang. Het artikel beoogt de vertrouwelijkheid van telecommunicatie te beschermen en het ongestoord functioneren van deze diensten te garanderen. Artikel 109 lid 2 bepaalt daarenboven dat aanbieders van telecommunicatiediensten die directe controle hebben over de communicatiesystemen, verplicht zijn om voldoende voorzorgsmaatregelen te treffen tegen storingen, aanvallen van buitenaf en de effecten van rampen. Dit dienen hoofdzakelijk maatregelen te zijn die de veiligheid van de data veiligstellen, het verlies of de beschadiging van data tegengaan en het misbruik van data voorkomt. Onder misbruik kan een aanval van buitenaf (bijvoorbeeld door hackers) of ongeautoriseerde toegang tot de data van werknemers worden verstaan. De veiligheidsmaatregelen dienen van geval tot geval te worden bepaald. Voor deze bepaling dient een veiligheidsconcept te worden voorgelegd aan de Duitse telecommunicatieautoriteit (artikel 109 lid 3 TKG). Een voorbeeld van een maatregel is het installeren van antivirus software of een beperking van de toegang tot ruimtes waar servers zijn opgesteld.

Verder schrijft artikel 4 van de richtlijn Privacy en elektronische communicatie voor dat gebruikers geïnformeerd dienen te worden over serieuze veiligheidsinbreuken. Dit voorschrift is niet in artikel 109 TGK geïmplementeerd. Artikel 93 lid 2 TGK bepaalt echter onder meer dat tussenpersonen hun gebruikers moeten inlichten over de veiligheidsrisico's van hun netwerken.

II. Toepassing bestaande regelgeving

Wettelijk kader

In Duitsland is er geen rechtspraak waarin de effectiviteit van de toepassing van het bestaande wettelijke kader aan bod is gekomen. De moeilijkheid met artikel 109 TGK is dat het bepaalde zorgplichten voor netwerk- en dienstenaanbieders in het leven roept, maar

geen minimum aan veiligheidsmaatregelen voorschrijft. Dit creëert onzekerheid bij de betrokken partijen.

III. Ontwikkelingen

Het Duitse *Verband der deutschen Internetwirtschaft e.V.*, (Vereniging van de Duitse Internet Economie, ECO) en het *Bundesamt für Informationssicherheit* (Federale Bureau voor Informatieveiligheid, BSI) zijn samen een anti-botnet project gestart. Het doel van het project is te komen tot een hulplijn die het publiek informeert over en computerhulp biedt bij het verwijderen van virussen en bots.[109] Tussenpersonen, zoals internetserviceproviders, hebben mogelijkheden om geïnfecteerde systemen te herkennen aan de hand van verdacht netwerkverkeer. De getroffen gebruiker kan dan op de hoogte worden gesteld van de besmetting. De gebruiker wordt geïnformeerd in een pop-up venster dat wordt geopend als de internetbrowser wordt gestart. De waarschuwing kan ook per gewone post worden verzonden. De anti-botnet website biedt daarna hulp in twee stappen. Eerst wordt de gebruiker met het besmette systeem doorverwezen naar een website waar de gebruiker informatie en software kan vinden om het probleem zelf te verhelpen. Mocht dit niet volstaan dan kan de gebruiker contact opnemen met een adviescentrum, dat de gebruiker hulp biedt bij het verwijderen van de kwaadaardige software en bij het voorkomen van toekomstige aanvallen. De gebruiker is echter niet verplicht deze maatregelen nemen. Hoewel het gaat om een samenwerking tussen de industrie en de Duitse overheid, zijn er geen dwangmiddelen beschikbaar die de gebruiker verplichten om actie te ondernemen.[110] ECO is namelijk uitsluitend verantwoordelijk voor de implementatie en de uitvoering van dit project. Men is niet van plan om verdergaande maatregelen te treffen, zoals het tijdelijk afsluiten van de internettoegang, wanneer een gebruiker nalaat om de adviezen op te volgen.[111]

De Duitse overheid benadrukt verder dat elke technologische maatregel om geïnfecteerde systemen op te sporen, dient te voldoen aan de bestaande Duitse dataprotectie regelgeving, in het bijzonder aan de regels inzake het (tele)communicatiegeheim.[112] Betrokken partijen hebben bevestigd dat deze eis de technologische mogelijkheid om geïnfecteerde systemen te detecteren beperkt.

[109] http://www.eco.de/verband/202_7268.htm.
[110] http://www.eco.de/verband/202_7268.htm.
[111] http://www.heise.de/security/meldung/Bundesweite-Zentrale-zur-Botnetz-Bekaempfung-wirft-Fragen-auf-882987.html.
[112] Ibid.

Kinderporno

I. Bestaande regelgeving

Wettelijk kader

Het bezit, het verspreiden en het tonen en maken van kinderporno wordt in Duitsland voornamelijk in artikel 184 van het *Strafgesetzbuch* (Duitse Strafwet, StGB) geregeld. Iedereen die jonger is dan 14 jaar wordt als kind beschouwd (artikel 176 StGB). Deze regelgeving is middels artikel 184c StGB ook van toepassing verklaard op de media en dus ook op het internet. Het gerechtshof in Hamburg heeft bepaald dat het enkele kijken naar kinderporno als een vorm van bezit van kinderporno dient te worden beschouwd. Daarvoor is het niet van belang dat het materiaal permanent op een harde schijf is opgeslagen.[113] Het verspreiden van kinderporno vangt aan wanneer de data de computer van de gebruiker binnenkomt. Het is daarbij niet van belang of de bron het materiaal heeft overgebracht of dat de ontvanger het materiaal heeft geopend.[114] Bovendien wordt aangenomen dat wanneer de data toegankelijk is, er sprake is van het tonen van kinderporno.[115]

Voorts zijn de in de inleiding genoemde bepalingen ter implementatie van de E-commerce richtlijn van toepassing.

Overige regulering

Naast de wettelijke regelingen en in het licht van de aansprakelijkheidsbeperking in de artikelen 7 tot en met 10 TMG zijn er andere maatregelen getroffen om kinderporno op het internet te reguleren. In het bijzonder met betrekking tot tussenpersonen bestaat er in Duitsland een systeem van non-gouvernementele organisaties die deel uitmaken van het INHOPE netwerk en naar de standaarden van INHOPE hotlines in het leven hebben geroepen. De Duitse organisaties die deelnemen in INHOPE zijn: *Electronic Commerce Forum* (ECO), *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* (FSM) en *jugendschutz.net*. FSM en ECO zijn daadwerkelijk relevant voor het reguleren van kinderporno.

De FSM is een in 1997 opgerichte organisatie van zichzelf regulerende Duitse multimedia-serviceproviders. De FSM is een van de organisaties die aan de wieg stonden van INHOPE en biedt een website waarop geklaagd kan worden over onrechtmatige online inhoud, zoals kinderporno.[116] Burgers kunnen hun beklag doen via een webformulier of e-mailadres.

[113] http://www.heise.de/newsticker/meldung/Urteil-Kinderpornos-anklicken-ist-strafbar-931446.html.
[114] BGH, NStZ 2001, 569.
[115] Ibid.
[116] http://www.fsm.de/de/Beschwerdeformular.

Wanneer de FSM een rapport ontvangt en de onrechtmatigheid is komen vast te staan, dan informeert de FSM de betrokken tussenpersoon over het onrechtmatige materiaal. De tussenpersoon dient dan binnen een vastgestelde periode te reageren op het bericht of moet het materiaal verwijderen. Wanneer niet op tijd tot actie wordt overgegaan, wordt een commissie van beroep op de hoogte gesteld en deze kan gepaste maatregelen nemen. Als het materiaal zijn oorsprong in het buitenland vindt, stuurt de FSM de klacht door naar INHOPE die op zijn beurt een andere partnerorganisatie op de hoogte brengt. Ongeveer 23% van het totaal aantal klachten heeft betrekking op kinderporno. FSM neemt geen klachten in behandeling die betrekking hebben op nieuwsgroepen.

ECO is een in 1993 opgerichte organisatie voor de Duitse interneteconomie. ECO biedt eveneens een hotline om onrechtmatig online materiaal te melden, vergelijkbaar met die van de FSM.
ECO biedt in samenwerking met de FSM een zogenaamde *Internetbeschwerdestelle* (internet klachten) hotline aan die tegelijk de officiële Duitse INHOPE klachtenlijn is.[117] Ook hier kunnen burgers via een webformulier melding maken van pornografisch materiaal op internet. Voor elke specifieke technologie (zoals websites, nieuwsgroepen, peer to peer-netwerken) bestaat een apart formulier. FSM en ECO delen samen de verantwoording voor de verschillende technologieën en sturen, afhankelijk van de technologie, klachten aan elkaar door.[118] Deze klachten worden dan intern afgehandeld door FSM of ECO en de betreffende tussenpersoon wordt door hen ingelicht wanneer het naar Duits recht onrechtmatig materiaal betreft. Wanneer het materiaal zijn oorsprong in het buitenland vindt dan wordt een INHOPE partnerorganisatie op de hoogte gebracht zodat actie ondernomen kan worden. Als er geen partnerorganisatie is dan wordt de buitenlandse tussenpersoon op de hoogte gesteld. Ook worden URL's, waarvan is vastgesteld dat ze onrechtmatig materiaal aanbieden, in een database opgeslagen om te voorkomen dat INHOPE organisaties geen overbodig werk doen.

De FSM legt tevens een code of conduct op aan al zijn leden. Alle grote internetserviceproviders en andere typen van tussenpersonen, zoals zoekmachines, zijn lid van de FSM. In onderdeel 1 van deze code is het doel van de code vastgesteld: het reguleren van onrechtmatig materiaal. In onderdeel 2 is bepaald dat leden ervoor zorgen dat kinderpornografisch materiaal niet wordt aangeboden of doorgegeven. Bovendien dienen leden de betreffende instanties te informeren wanneer zij kinderpornografisch materiaal ontdekken.

[117] http://www.internet-beschwerdestelle.de/index.htm.
[118] FSM is verantwoordelijk voor informatie op het World Wide Web, inhoud voor mobiele telefoons die via internet toegankelijk is, leeftijdsverificatie systemen en chat. ECO is verantwoordelijk voor nieuwsgroepen, spam/e-mail, ICRA-labels en peer to peer-netwerken. http://www.internet-beschwerdestelle.de/beschwerde /verfahrensordnung/index.htm.

II. Toepassing bestaande regelgeving

Wettelijk kader

De regelgeving in de TMG is effectief als het gaat om inhoud in het publieke domein en kunnen dus worden opgemerkt door derden die een tussenpersoon kunnen informeren. Het betreft dan veelal websites, terwijl het overgrote deel van het kinderpornografische materiaal wordt verspreid via beschermde kanalen als peer to peer-netwerken, BitTorrent en gesloten nieuwsgroepen. Daarnaast begrenst het communicatiegeheim de mogelijkheden die tussenpersonen hebben bij de uitvoering van bepaalde technologische maatregelen, zoals het blokkeren van IP adressen. De impact en effectiviteit van dit aansprakelijkheidsregime is daarom beperkt.

Overige regulering

FSM en ECO bieden het Duitse publiek een helder hotline systeem voor het aangeven van kinderpornografisch materiaal. Het systeem biedt een snelle en praktische methode voor het verwijderen van kinderporno die publiekelijk toegankelijk is. Bovendien beschermen de FSM en ECO hotlines onder meer internetserviceproviders tegen klachten over kinderpornografisch materiaal. Er bestaan echter geen openbare statistische gegevens met betrekking tot het type materiaal dat is geblokkeerd en ook de wijze waarop wordt geëvalueerd is onbekend. Hierdoor is een gebrek aan transparantie ontstaan. Tevens is het daarom moeilijk om de effectiviteit van de systemen te meten.

III. Ontwikkelingen

Er is in Duitsland een nieuwe wet aangenomen om kinderporno te reguleren.[119] Het *Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen* (Wet die de toegang tot kinderporno via communicatienetwerken bemoeilijkt, Zugangserschwerungs-gesetz – ZugErschwG) werd in 2009 opgesteld op initiatief van Ursula von der Leyen, de toenmalige minister van gezin. Het doel van de wet is de toegang tot kinderpornografisch materiaal op internet lastiger te maken. Om dit doel te bereiken dient het *Bundeskriminalamt* (BKA) krachtens artikel 1 ZugErschwG een lijst op te stellen van domeinnamen, IP adressen en URL's van websites die kinderporno bevatten of linken naar websites met materiaal van kinderpornografische aard. De lijst moet dagelijks vernieuwd worden. Internetserviceproviders die meer dan 10.000 afnemers hebben zijn verplicht om de toe-

[119] http://www2.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl.

gang tot deze websites ten minste op DNS-niveau te blokkeren. Gebruikers die proberen toegang tot deze websites te krijgen, dienen te worden doorgeleid naar een website van het BKA met daarop een stopteken en een korte uitleg dat de browser heeft geprobeerd om inhoud te bereiken die door het BKA als kinderporno is aangemerkt.[120] Internetservice-providers dienen geanonimiseerde bezoekersstatistieken van deze website op te maken en aan het BKA te overhandigen. Daarnaast heeft de Duitse overheid een contract gesloten met vijf grote internetserviceproviders over het blokkeren van kinderpornografisch materiaal. Deze contracten werden steeds apart met een internetserviceprovider uitonderhandeld en de inhoud ervan wordt geheim gehouden. Zelfs de betrokken internetserviceproviders zijn onderling niet op de hoogte van de inhoud van elkaars contracten.

Echter, de wet is omstreden en de vraag was zelfs of de wet wel moest worden doorgezet. Evenwel, op 17 februari 2010 werd de wet door de Duitse bondspresident onverwachts ondertekend en trad zij vervolgens in werking.[121] De overheid heeft nu echter ingestemd met het niet opstellen van een zwarte lijst door het BKA, noch tot het doen van verzoeken aan internetserviceproviders om de toegang tot bepaalde inhoud te blokkeren.[122] Ook is de intrekking van de wet of het vervangen ervan onderwerp van debat.

[120] http://de.wikipedia.org/w/index.php?title=Datei:Kinder_stopp.png&filetimestamp= 20090418174246.
[121] Zie voetnoot 9.
[122] http://www.heise.de/newsticker/meldung/Justizministerium-hofft-bei-Websperren-auf-abgerundete-Loesung-937249.html.

Auteursrecht

I. Bestaande regelgeving

Wettelijk kader

Het gebruik, het kopiëren en de verspreiding van auteursrechtelijk beschermd materiaal is hoofdzakelijk geregeld in het Duitse *Gesetz über Urheberrecht und verwandte Schutzrechte* (Auteurswet, Urheberrechtsgesetz – UrhG). De wet werd in 1965 aangenomen maar is daarna vaak geamendeerd in het licht van technologische ontwikkelingen. Verder kunnen nog worden genoemd het *Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft* en *Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums*.

Artikelen 15 tot en 24 UrhG geven de makers van literaire, dramatische, muzikale en artistieke werken het uitsluitend recht om te bepalen hoe en of hun werk gekopieerd, verspreid en tentoongesteld mag worden. De implementatie van de Auteursrechtrichtlijn heeft daarbij het UrhG aangepast aan nieuwe telecommunicatie technologieën. Artikel 19a UrhG bepaalt dat de rechthebbende ook het uitsluitende recht heeft om zijn werk openbaar te maken. Er is sprake van openbaar maken wanneer het materiaal wordt overgebracht via een bedrade of draadloze verbinding op een door de gebruiker gekozen tijdstip en plaats. Het dient opgemerkt te worden dat het kopen van een informatiedrager niet met zich meebrengt dat het materiaal daarop openbaargemaakt mag worden. Ingevolge artikel 53 UrhG is het downloaden van auteursrechtelijk beschermd materiaal onrechtmatig wanneer het kopiëren van het openbaargemaakte materiaal kennelijk onrechtmatig is. Artikel 53 UrhG regelt het rechtmatig kopiëren van auteursrechtelijk beschermd materiaal voor privégebruik. Verder biedt de regelgeving verschillende middelen aan rechthebbenden om de rechten, zoals gedefinieerd in artikelen 15 tot en met 24 UrhG, te beschermen. Artikel 97 UrhG geeft rechthebbenden het recht om inbreukmakend materiaal te verwijderen en een gebods- of verbodsactie in te stellen.

Artikelen 7 tot en met 10 TMG regelen, zoals eerder aangegeven, de verantwoordelijkheden van tussenpersonen, waaronder ook ook hun verantwoordelijkheden op auteursrechtelijk gebied vallen.

Overige regulering

De hierboven beschreven wettelijke bepalingen zijn in Duitsland het uitgangspunt voor het reguleren van auteursrechtinbreuk op het internet. In tegenstelling tot kinderporno, zijn er geen ECO of FSM hotlines die voor tussenpersonen zorgplichten met betrekking tot auteursrechtinbreuk in het leven roepen.

II. Toepassing bestaande regelgeving

Wettelijk kader

Volgens de heersende leer worden zowel het publiekelijk online aanbieden van materiaal als de overbrenging ervan als openbaar maken aangemerkt. Het is daarbij niet van belang of het materiaal daadwerkelijk ontvangen is.[123] Zo leidt het aanbieden en delen van auteursrechtelijk beschermd materiaal op peer-to-peer netwerken tot een schending van artikel 19a UrhG.[124]

Er is in Duitsland discussie over de vraag of, ondanks de inperkingen als geregeld in de artikelen 7 tot en met 10 TMG, gebods- of verbodsacties tegen internetserviceproviders en andere tussenpersonen zijn in te stellen. Dit zou kunnen wanneer het handelen van een tussenpersoon ingevolge artikelen 823 en 1004 *Bürgerliches Gesetzbuch* wordt aangemerkt als een indirecte auteursrechtinbreuk. Iemand die een indirecte auteursrechtinbreuk pleegt (een *Störer*), neemt opzettelijk deel in het veroorzaken of het in standhouden van een inbreuk. Internetserviceproviders die toegang tot het internet aanbieden nemen het risico dat hun gebruikers hun faciliteiten gebruiken voor het plegen van auteursrechtinbreuk. Het is dan gerechtvaardigd om internetserviceproviders aan te merken als *Störer*. Een indirecte auteursrechtinbreuk vereist echter het niet nakomen van zorgplichten tot onderzoek (*Prüfplichten*). Deze zorgplichten komen niet overeen met de zorgplicht om netwerkverkeer te controleren waarvan internetserviceproviders zijn vrijgesteld op basis van artikel 7 TMG. Omdat het om andere zorgplichten gaat kunnen internetservice-providers, ondanks de aansprakelijkheidsvermindering, als indirecte inbreukmakers worden aangemerkt. De zorgplichten tot onderzoek worden niet nageleefd wanneer de zorgplicht redelijkerwijs van de indirecte inbreukmaker verwacht mag worden. Of hiervan sprake is als het gaat om internetserviceproviders is controversieel. In ieder geval worden de zorgplichten tot onderzoek beperkt door het (tele)communicatiegeheim van artikel 88 TKG (artikel 7 TMG). Het (tele)communicatiegeheim is van toepassing op de inhoud van de telecommunicatie en verkeersgegevens, zoals IP adressen en de opgevraagde webpagina's. Met andere woorden: de informatie die nodig is om vast te stellen of er sprake is van auteursrechtinbreuk. Internetserviceproviders zijn daarom niet in staat om te voldoen aan de zorgplichten zonder het (tele)communicatiegeheim te schenden. Zij kunnen daarom geen indirecte auteursrechtinbreuk plegen en rechthebbenden kunnen tegen hen geen gebod- of verbodsacties instellen.[125]

[123]Gercke (2006).
[124]Gercke (2009).
[125]Gercke (2006)

Identiteitsfraude

I. Bestaande regelgeving

Wettelijk kader

Identiteitsfraude is als zodanig niet wettelijk geregeld. Sommige strafbaar gestelde online feiten hebben een element dat raakt aan identiteitsfraude, bijvoorbeeld phishing dat strafbaar is gesteld in het Duitse *Strafgesetzbuch* (StGB, Wetboek van Strafrecht).

II. Toepassing van bestaande regelgeving

Wettelijk kader

Dat identiteitsfraude niet strafbaar is naar Duits recht is ook in de jurisprudentie bevestigd ten aanzien van online activiteiten, bijvoorbeeld in een zaak, waarin de rechter vaststelde dat het registreren en handelen op eBay onder een valse identeit niet onrechtmatig is.[126]

Hoewel de relevantie van het StGB voor online criminaliteit in het verleden onderwerp van discussie was, is de meerderheid van auteurs het er nu over eens dat artikel 269 StGB, dat het vervalsen van bewijsmiddelen strafbaar stelt, ook van toepassing is op frauduleuze activiteiten als *phishing*.[127]

[126] http://www.telemedicus.info/urteile/Internetrecht/899-KG-Berlin-Az-4-1-Ss-18109-13009-Strafbarkeit-der-Anmeldung-bei-eBay-unter-falschem-Namen.html.

[127] See e.g., A. Seidl, K Fuchs, "Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes" (2010) 2 HRRS, 85; M. Gercke, "Die Strafbarkeit von "Phishing" und Identitätsdiebstahl - Eine Analyse der Reichweite des geltenden Strafrechts", (2005) CR, 606 ff.

Verkoop gestolen goederen

I. Bestaande regelgeving

Wettelijk kader

De verkoop van gestolen goederen (*Hehlerei*) is in Duitsland in het StGB verboden. Artikel 259 StGB definieert heling als het verwerven, kopen of het anderszins in bezit krijgen van, of een ander voorzien van of met winst verkopen aan een ander van een goed dat door een derde is gestolen of anderszins is verworven door een inbreuk op het eigendomsrecht van een ander. Het is van belang om de handel van goederen die eerder zijn gestolen te onderscheiden van de handel in goederen die inbreuk maken op intellectuele eigendomsrechten.

Overige regulering

Er is in Duitsland geen vorm van specifieke (zelf)regulering in verband met de verkoop van gestolen goederen. Wel kennen platformaanbieders eigen regels die zij toepassen om de verkoop van gestolen goederen tegen te gaan.

II. Toepassing bestaande regelgeving

Wettelijk kader

Ofschoon het niet de positie van internetservice providers betreft, is het interessant om te vermelden dat het *Bundesgerichtshof* in drie verschillende zaken heeft bepaald dat online veiligwebsites – in tegenstelling tot internetserviceproviders en andere tussenpersonen – indirect aansprakelijk zijn voor namaakgoederen (*Störerhaftung*).[128] Een en ander brengt verder met zich mee dat veilingwebsites een zorgplicht hebben om toekomstige inbreuken op intellectueel eigendomsrecht door gebruikers, die reeds als potentiële inbreukmakers zijn aangemerkt, te voorkomen. Het hof heeft bepaald dat het gebruik van filtersoftware hierbij kan helpen en dat zulke maatregelen niet onproportioneel zijn.

Overige regulering

Voor wat betreft de positie van platformaanbieders kan worden verwezen naar wat eerder is opgemerkt over de eigen interne procedures van partijen als eBay.

[128] BGH Urteil: 11.03.2004 Az. I ZR 304/01; 19.04.2007 Az. I ZR 35/04; 12.07.2007 - Az. I ZR 18/04.

Frankrijk

Inleiding

Wettelijk kader

De artikelen 12 tot en met 15 van de E-commerce richtlijn zijn geïmplementeerd in de *Loi pour la confiance dans l'économie numérique*[129] (LCEN). Zoals later zal worden aangegeven, is de reikwijdte van LCEN aanzienlijk groter dan de reikwijdte van de E-commerce richtlijn. Artikel 6 en artikel 9 van deze wet regelen de aansprakelijkheid van internetservice-providers ten aanzien van mere conduit, caching en hosting activiteiten. Hierbij moet worden opgemerkt dat artikel 6 verder niet nader is geïncorporeerd in een wetboek; terwijl artikel 9 nader is geïncorporeerd in artikel L. 32-3-3 en artikel L. 32-3-4 van de *Code des postes et communications électroniques* (CPCE). Artikel 6 maakt echter wel onderdeel uit van de Franse wetgeving als artikel in de LCEN.

Overeenkomstig de E-commerce richtlijn maakt de Franse wetgeving een onderscheid tussen de drie activiteiten: mere conduit (artikel 6-I-1 LCEN en artikel L. 32-3-3 CPCE); caching (artikel L.32-3-4 CPCE) en hosting (artikel 6-I-2 LCEN). Artikel 15 van de E-commerce richtlijn, inhoudende het verbod op een algemene toezichtverplichting, is geïmplementeerd in artikel 6-I-7 LCEN.

Op grond van artikel L.32-3-3 CPCE is een dienstenaanbieder van mere conduit activiteiten (het onverkort doorgeven/toegang verschaffen van informatie) alleen aansprakelijk indien (a) het initiatief tot de doorgifte bij de dienstenaanbieder ligt; (b) de ontvanger van de doorgegeven informatie door de dienstenaanbieder wordt geselecteerd; of (c) de doorgegeven informatie door de dienstenaanbieder wordt geselecteerd of gewijzigd. Op grond van artikel L. 32-3-4 CPCE is een dienstenaanbieder van caching activiteiten (de automatische, tussentijdse en tijdelijke opslag van informatie met het enkele doel de doeltreffendheid van de doorgifte te verbeteren), gevrijwaard van civielrechtelijke en strafrechtelijke aansprakelijkheid voor de opgeslagen informatie. De vrijwaring van aansprakelijkheid vervalt echter indien de dienstenaanbieder de informatie wijzigt, de toegangsvoorwaarden voor de informatie of de gangbare regels betreffende de bijwerking van de informatie niet in acht neemt, of in strijd handelt met het alom erkende en in de bedrijfstak gangbare rechtmatige gebruik van technologie voor het verkrijgen van gegevens over het gebruik van de informatie.

[129] Loi n° 2004-575 du 21 juin 2004, JORF n° 143 du 22 juin 2004, p. 11168.

Een dienstenaanbieder van caching activiteiten is eveneens aansprakelijk indien de dienstenaanbieder niet prompt handelt om de door hem opgeslagen informatie te verwijderen of de toegang daartoe onmogelijk te maken (a) zodra hij er daadwerkelijk kennis van heeft dat de informatie verwijderd is dan wel dat de toegang daartoe onmogelijk is gemaakt op de plaats waar de informatie zich oorspronkelijk in het net bevond; of (b) indien een rechtbank heeft bevolen de informatie te verwijderen of de toegang daartoe onmogelijk te maken.

Artikel 6-I-2 LCEN definieert een dienstenaanbieder van hosting activiteiten als een natuurlijk persoon of rechtspersoon die de opslag van signalen, tekst, afbeeldingen, geluid en berichten van iedere aard voor het publiek toegankelijk maakt. Een dienstenaanbieder van hosting activiteiten is gevrijwaard van civielrechtelijke aansprakelijkheid indien de dienstenaanbieder (a) niet daadwerkelijk kennis heeft van de onwettige aard van de opgeslagen informatie of van feiten en omstandigheden waaruit de onwettige aard van de informatie blijkt; of (b) zodra hij van het bovenstaande in kennis wordt gesteld, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken. Op grond van artikel 6-I-3 LCEN is de dienstenaanbieder van hosting activiteiten onder dezelfde voorwaarden eveneens gevrijwaard van strafrechtelijke aansprakelijkheid, met dien verstande dat de dienstenaanbieder wel strafrechtelijk aansprakelijk is indien het kennis heeft van de onwettige activiteit of informatie en niet van de onwettige aard van de activiteit of informatie.

Artikel 6-I-5 LCEN roept een optionele notificatieprocedure in het leven, op basis waarvan de dienstenaanbieder wordt verondersteld daadwerkelijk kennis te hebben van het feit dat onwettige inhoud bij hem staat opgeslagen. Deze procedure valt buiten de reikwijdte van de E-commerce richtlijnen en vereist dat de notificatie de volgende elementen bevat: datum, beschrijving van de feiten en de exacte locatie, redenen voor de verwijdering en een kopie van de brief die naar de maker of bewerker van het materiaal is verzonden met het verzoek de onwettige activiteit te stoppen. Artikel 6-I-5 LCEN vormt dus in samenhang met de artikelen 6-I-2 en 6-I-3 LCEN de Franse 'notice and takedown' procedure.

Tot slot hebben de lidstaten op grond van artikel 15 van de E-commerce richtlijn de mogelijkheid om de dienstenaanbieders te verplichten om de bevoegde autoriteiten, op verzoek, onverwijld te voorzien van informatie over de afnemers van hun dienst met wie zij opslagovereenkomsten hebben gesloten, op basis waarvan deze afnemers kunnen worden geïdentificeerd. Op grond van de eerste paragraaf van artikel 6-II LCEN zijn zowel internetserviceproviders als dienstenaanbieders die hosting activiteiten aanbieden (dit kunnen uiteraard ook internetserviceproviders zijn) verplicht om informatie op te slaan die het mogelijk maakt om een ieder die heeft bijgedragen aan de opslag of het doorgeven van informatie te kunnen identificeren. De derde paragraaf van artikel 6-II LCEN stelt de bevoegde autoriteiten in staat om deze informatie op te vragen. Een nadere definiëring om wat voor informatie het precies gaat en de exacte bewaartermijn die zou gelden voor deze informatie zou moeten volgen uit een verordening die er op dit moment nog niet is.

Rechtbanken maken regelmatig gebruik van dit artikel om identificerende informatie over de maker van de betwiste opgeslagen informatie op te vragen bij dienstverleners van hostingactiviteiten.

Internetveiligheid

I. Huidige regelgeving

Wettelijk kader

Artikel D.98-5 CPCE en artikel 34 van de *Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés*[130] (Loi Informatique et Libertés) reguleren de technische integriteit en veiligheid van openbare elektronische telecommunicatienetwerken en -diensten.

Artikel D.98-5 CPCE is de Franse implementatie van artikel 4 van de richtlijn Privacy en elektronische communicatie. Op grond van artikel D.98-5 CPCE is de aanbieder van een openbaar elektronisch telecommunicatienetwerk verplicht om alle noodzakelijke maatregelen te treffen om de veiligheid van de communicatie over zijn netwerk te garanderen. De noodzakelijke technische maatregelen worden vastgesteld door de Autorité de Régulations des Communications Electroniques et des Postes (ARCEP), de Franse toezichthouder op het gebied van telecommunicatie en post. ARCEP kan op vertrouwelijke basis in kennis worden gesteld van de maatregelen die de aanbieders hebben genomen om de veiligheid van hun netwerk te garanderen. De aanbieder heeft de plicht om de abonnees te informeren over diensten die de veiligheid van het netwerk kunnen vergroten. Daarnaast heeft hij de plicht om de abonnees te informeren over bijzondere risico's inzake inbreuken op de veiligheid en over de eventuele middelen om deze risico's tegen te gaan met inbegrip van een indicatie van de verwachte kosten. Aanbieders van openbare elektronische communicatienetwerken – waarop de verplichtingen van artikel D.98-5 CPCE betrekking hebben – zijn volgens artikel 32 (15°) CPCE natuurlijke of rechtspersonen die een voor het publiek toegankelijk elektronisch communicatienetwerk exploiteren en elektronische communicatiediensten aanbieden. Ingevolge artikel 32 (6°) CPCE vallen uitgeversactiviteiten of distribuerende activiteiten van openbare elektronische communicatiediensten via elektronische weg niet onder deze definitie. Volgens de interpretatie van ARCEP, vallen internetserviceproviders onder de definitie van artikel 32 (15°) CPCE, omdat zij als toegangsdienst een dienst leveren die de doorgifte van elektronische communicatie mogelijk maakt.[131] Zodoende zijn marktpartijen die niet actief zijn in het uitzenden, doorgeven en ontvangen van geluid, signalen of afbeeldingen zijnde elektronische communicatie – zoals dienstenaanbieders van hostingactiviteiten – uitgesloten van het toepassingsbereik van artikel D.98-5 CPCE.

---

[130] Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, verschillende malen geamendeerd en beschikbaar via : http://www.cnil.fr/en-savoir-plus/textes-fondateurs/.

[131] La lettre de l'Autorité de Régulation des Télécommunications, n° 41, Novembre/Décembre 2004, p.11 'Qu'est-ce qu'un opérateur de communications électroniques ?', beschikbaar via: http://www.arcep.fr/fileadmin/reprise/communiques/lettre/pdf/lettre41-p11.pdf.

Overige regulering

In de strijd tegen spam is er een nationaal meldpunt, 'Signal Spam', opgezet door diverse overheidsinstanties, private partijen en andere organisaties. Het doel van dit meldpunt is om internetgebruikers te informeren over de verschillende vormen van spam (waaronder phishing) en om te strijden tegen de verspreiding ervan, door middel van het identificeren van de servers die spam versturen en 'zombie PCs'. Internetgebruikers kunnen zich via de website www.signal-spam.fr registreren en een plug-in downloaden om ongevraagde e-mailberichten direct door te sturen naar het meldpunt. Daarnaast kan men via een formulier op de website meldingen van spam aan het meldpunt doorgeven. Na ontvangst analyseert Signal Spam de meldingen van gebruikers en stuurt ze deze vervolgens door naar de bevoegde autoriteiten. Die kunnen vervolgens een onderzoek starten en sancties opleggen.

Het probleem van ongevraagde communicatie is niet een recent probleem in Frankrijk. In 2002 heeft AFA, de organisatie die de belangen van internetserviceproviders vertegenwoordigt, zijn 'professional practices' aangepast en internetserviceproviders aanbevolen om technische maatregelen te nemen om spam te detecteren en de verzending van spam onmogelijk te maken.[132] Daarnaast heeft AFA specifieke aanbevelingen op haar website gepubliceerd, gericht aan internetserviceproviders, aanbieders van e-mailsoftware en aanbieders van e-maildiensten, hoe zij spam kunnen bestrijden. De aanbevelingen zien onder meer op de bescherming van de computers van eindgebruikers tegen aanvallen van buitenaf en het detecteren van 'zombie PCs'.[133]

II. Toepassing van de regelgeving

Wettelijk kader

Artikel D.98-5 CPCE bevat geen specifieke sanctiebepaling indien aanbieders van elektronische communicatienetwerken zich niet houden aan hun zorgplicht. Op grond van artikel L.36-11 CPCE is ARCEP bevoegd om sancties op te leggen indien de aanbieders hun verplichtingen niet vervullen. Afhankelijk van de ernst van het niet nakomen van een plicht kan ARCEP het recht om een openbaar elektronisch communicatienetwerk te vestigen of om een openbaar elektronische communicatiedienst aan te bieden, gedeeltelijk dan wel volledig voor maximaal een maand opschorten. ARCEP heeft ook de mogelijkheid om boetes op te leggen. ARCEP is dus krachtens artikel L.36-11 CPCE bevoegd om sancties en boetes op te leggen aan internetserviceproviders die niet de geschikte

[132] Pratiques et Usages, les principes communs aux membres de l'AFA: www.afa-france.com/deontologie.html.
[133] Lutte contre le spam : http://www.afa-france.com/t_spam.html.

beveiligingsmaatregelen hebben getroffen. Uit de interviews kwam naar voren dat beveiligingslekken in Frankrijk worden gekwalificeerd als staatsgeheim (*secret défense*). Dergelijke lekken zijn dus vertrouwelijk en kunnen alleen worden bekend gemaakt aan de daartoe geautoriseerde partijen. Op dit moment is ARCEP nog niet geautoriseerd om dergelijke informatie over beveiligingslekken te ontvangen. Het probleem van beveiligingslekken zal moeten worden aangepakt door het Ministerie van Defensie, via de gespecialiseerde Franse inlichtingendienst *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI). Er is zeer weinig informatie beschikbaar over de rol van ANSSI inzake beveiligingslekken. De inlichtingendienst heeft wel een eigen website over computerbeveiliging (www.securite-informatique.gouv.fr), waarop zij technische adviezen en 'good practices' publiceert over de bescherming van computers van individuen en bedrijven.

Overige regulering

Volgens het jaarrapport van 'Signal Spam' over 2007-2008[134], zijn er in deze periode in totaal 14 miljoen meldingen van spam binnengekomen en hebben 48 500 gebruikers zich geregistreerd. Er is geen informatie beschikbaar over de effectiviteit van dit systeem, in het bijzonder over de hoeveelheid technische middelen en arbeidsuren die beschikbaar worden gesteld om het hoge aantal meldingen te kunnen verwerken. Op basis van de interviews komt naar voren dat Signal Spam niet de gemelde spamberichten zelf beoordeelt, maar deze op basis van samenwerkingsovereenkomsten doorstuurt naar de relevante bevoegde autoriteiten. Zo heeft bijvoorbeeld de CNIL na het aangaan van een samenwerkingsovereenkomst met Signal Spam in september 2008 een aantal controles op locatie uitgevoerd om te controleren of online marketingdiensten zich wel aan de wet houden.

III. Ontwikkelingen

Twee senatoren hebben namens de Senaatscommissie van wetgeving in mei 2009 een rapport (*Rapport d'information sur la vie privée à l'heure des mémoires numériques)* gepubliceerd over het recht op privacy in tijden van digitale opslag.[135] In dit rapport wordt onder andere aanbevolen om een nieuwe meldplicht jegens CNIL voor beveiligingslekken in te voeren.

---

[134] Rapport d'activité 2007-2008, Signal Spam, beschikbaar via: https://www.signal-spam.fr/Rapport2008-VF.pdf.

[135] 'La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information', Rapport d'Information n° 441 (2008-2009), M. Yves Détraigne et Mme Anne-Marie Escoffier, fait au nom de la Commission des lois, 27 mei 2009, beschikbaar via: http://www.senat.fr/noticerap/2008/r08-441-notice.html.

Op basis van dit rapport hebben de twee senatoren op 9 november 2009 een wetsvoorstel ingediend om het recht op privacy in de digitale omgeving beter te waarborgen.[136] Artikel 7 van dit wetsvoorstel beoogt om artikel 34 *Loi Informatique et Libertés* te amenderen en zou in zijn huidige vorm een voorlopige (gedeeltelijke) implementatie zijn van het recentelijk uitgebreide artikel 4 van de Richtlijn privacy en elektronische communicatie. Het voorgestelde gewijzigde artikel 34 luidt: *De voor de verwerking verantwoordelijke zal alle nodige maatregelen treffen (…) om de veiligheid van data te waarborgen en persoonsgegevens te beschermen tegen onvoorziene of onwettige vernietiging, verlies, wijziging, openbaarmaking, doorgifte, opslag, verwerking of ongeautoriseerde of onwettige toegang, in het bijzonder wanneer de verwerking de doorgifte van persoonsgegevens over een netwerk impliceert als ook tegen iedere vorm van onwettige verwerking. In het geval van een inbreuk in verband met persoonsgegevens zal de voor de verwerking verantwoordelijke onverwijld haar privacyfunctionaris hiervan op de hoogte stellen of, indien niet aanwezig, stelt zij de CNIL hiervan op de hoogte. Indien de inbreuk in verband met persoonsgegevens de persoonsgegevens van een of meerdere natuurlijke personen treft dan zal de voor de verwerking verantwoordelijke hen daarover in kennis stellen.* De inhoud, vorm en formaliteiten van deze meldplicht zal bij besluit nader moeten worden gespecificeerd.

Er dient te worden opgemerkt dat het huidige artikel 34 *Loi Informatique et Libertés* reeds voorziet in een vergelijkbare verplichting ten aanzien van de veiligheid en integriteit van data. Het nieuwe element dat in het wetsvoorstel wordt geïntroduceerd is de meldplicht voor inbreuken in verband met persoonsgegevens. Dit element komt overeen met het recentelijk uitgebreide artikel 4 van de Richtlijn privacy en elektronische communicatie, terwijl andere elementen van het wetsvoorstel afwijken van artikel 4.

Ten eerste legt de Richtlijn privacy en elektronische communicatie de beveiligingsverplichtingen ten aanzien van persoonsgegevens alleen op aan aanbieders van openbare elektronische communicatiediensten, zoals internetserviceproviders. De tekst van de Franse implementatie ziet op de voor de verwerking verantwoordelijke natuurlijke persoon of rechtspersoon. Deze categorie is veel breder dan de categorie van de Richtlijn. Ten tweede, artikel 4 spreekt alleen over een meldplicht jegens de bevoegde nationale autoriteiten. In het wetsvoorstel is dit vertaald naar een meldplicht jegens de CNIL. Het was tevens relevant geweest als men had onderzocht of de ANSSI niet een rol zou moeten spelen in de veiligheid van dataverwerking, gezien haar takenpakket als nationale autoriteit voor de veiligheid van informatiesystemen.[137] Het wetsvoorstel is tijdens de sessie van 23 maart 2010 door de *Sénat* behandeld en doorverwezen naar de *Assemblée nationale*.[138]

---

[136] 'Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique', n°93, door M. Yves Détraigne en Mme Anne-Marie Escoffier, 6 november 2009, beschikbaar via: http://www.senat.fr/leg/ppl09-093.html.

[137] Coupez (2010) .

[138] 'Proposition de loi , adoptée par le Sénat, visant à mieux garantir le droit à la vie privée à l'heure du numérique', n° 2387, 24 maart 2010, beschikbaar via: http://www.assemblee-nationale.fr/13/dossiers/vie_privee_numerique.asp.

Kinderporno

I. Huidige regelgeving

Wettelijk kader

De wettelijke bepalingen die kinderporno reguleren kan men in Frankrijk vinden in artikel 227-23 *Code pénal*, het Franse wetboek van strafrecht. In dit artikel worden vier strafbepalingen gedefinieerd. De verspreiding, vastlegging, opname en doorgifte van beeldmateriaal van een minderjarige is strafbaar indien het beeldmateriaal pornografisch van aard is. Het aanbieden, beschikbaar stellen en distribueren van dergelijk materiaal langs iedere weg dan wel het importeren en exporteren van dit materiaal is eveneens strafbaar. De straffen en boetes worden verhoogd indien een elektronisch communicatienetwerk wordt gebruik om het beeldmateriaal van de minderjarige te distribueren naar een onbepaald publiek. Tot slot is het regelmatig raadplegen van dergelijke openbare elektronische communicatiediensten waarop dergelijk materiaal wordt afgebeeld, of het verbergen van dergelijk materiaal ook strafbaar.[139]

Ten aanzien van de doorgifte en opslag van kinderporno is voor internetserviceproviders het aansprakelijkheidsregime van de in de inleiding beschreven *Loi pour la confiance dans l'économie numérique* (LCEN) van toepassing. Daarnaast bevat de LCEN bepalingen die zien op specifieke onwettige informatie zoals vermeld in artikel 6-I-7, derde paragraaf LCEN. Het op deze lijst vermelde materiaal wordt als zeer schadelijk beschouwd en wordt algemeen omschreven als *contenus odieux*.[140] Binnen deze categorie valt materiaal inzake misdrijven tegen de menselijkheid, rassenhaat, kinderporno, aanzetten tot geweld of dat de menselijke waardigheid aantast. Voor dit type materiaal hebben de internetserviceproviders en aanbieders van hostingdiensten de plicht om een gemakkelijk toegankelijke en zichtbare procedure (*procédure de signalement*) op te zetten die een ieder in staat stelt om de aanwezigheid van dit soort materiaal te melden aan de internetserviceprovider en/of aanbieder van hostingdiensten. Nadat zij op de hoogte zijn gesteld moeten de internetserviceproviders en/of aanbieders van hostingdiensten de bevoegde autoriteiten (o.a. het Centraal Bureau

[139] Artikel 227-22-1 stelt eveneens het benaderen van een minderjarige tot 15 jaar (of iemand die zich als zodanig voordoet) door een meerderjarige tot het aangaan van seksueel contact via een communicatienetwerk, strafbaar.

[140] « Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » nº 627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 januari 2008. Beschikbaar via: http://www.assemblee-nationale.fr/13/rap-info/i0627.asp.

tegen cybercriminaliteit (OCLCTIC)[141], het onderzoeksteam op het gebied van IT-fraude[142], de politie, de gendarmerie en de openbare aanklager) notificeren. Op grond van artikel 6-I-2 LCEN hoeven alleen aanbieders van hostingdiensten dit onmiskenbaar onrechtmatig materiaal te verwijderen nadat zij van de aanwezigheid hiervan in kennis zijn gesteld. Internetserviceproviders (indien zij alleen toegangsdiensten verlenen) zijn hiertoe alleen verplicht nadat de rechtbank hen hiertoe heeft bevolen.

Overige regulering

In de strijd tegen kinderporno is een aantal initiatieven gestart via coregulering/zelfregulering.

In 1998 heeft *AFA*, een organisatie die de Franse aanbieders van toegangs- caching- en hostingdiensten vertegenwoordigt, een meldpunt (www.pointdecontact.net) in het leven geroepen tegen *illegaal materiaal inhoudende kinderporno, rassenhaat, vergoelijking en aanzetten tot misdaden tegen personen, terrorisme of het provoceren tot zelfmoord.*[143] *Point de Contact* is het Franse lid van de Europese meldpuntorganisatie, INHOPE. In 2004 heeft AFA een gedragscode ontwikkeld die door de vertegenwoordigde internetserviceproviders is ondertekend. De gedragscode (*Charte contre les contenus odieux)* ziet op materiaal dat schadelijk is voor de menselijke waardigheid en bevat bepalingen over kinderporno.

Artikel 2 van de gedragscode herinnert de internetserviceproviders aan hun wettelijke verplichting (artikel 6-I-7 LCEN) om te voorzien in een meldingssysteem, en stelt voor om gebruik te maken van de gecentraliseerde *Point de Contact*. Internetserviceproviders zijn overeengekomen dat zij hyperlinks naar het notificatieformulier van *Point de Contact* plaatsen op o.a. hun fora, chat rooms en hun homepage, zodat internetgebruikers met een klik onwettig materiaal kunnen melden. Daarnaast zijn internetserviceproviders overeengekomen om de informatie voor ouders hoe zij hun kinderen kunnen beschermen gemakkelijk toegankelijk te maken en hebben ze voorgesteld om filtersoftware en andere toepassingen ter handhaving van ouderlijk gezag gratis ter beschikking te stellen. Volgens artikel 3 zullen internetserviceproviders direct of via de *Point de Contact* de handhavende autoriteiten prompt in kennis stellen van het onwettige materiaal. Tevens zijn ze overeengekomen om het onwettige materiaal prompt te verwijderen dan wel de toegang daartoe te blokkeren. Op grond van artikel 4 van de gedragscode zijn internetservice-providers overeengekomen om samen te werken met de rechterlijke autoriteiten door bepaalde informatie op te slaan die het mogelijk maakt om de maker van het materiaal of de gebruikers van de diensten van de internetserviceprovider te identificeren. Zij geven eveneens wijzigingen in de contactgegevens door aan de bevoegde autoriteiten en werken

[141] Office Central de Lutte contre la Criminalité Liées aux Technologies de l'Information et de la Communication.
[142] Brigade d'enquêtes sur les fraudes aux technologies de l'information, BEFTI.
[143] AFA's Annual Report, March 2008-June 2009.

mee om gericht en tijdelijk de informatie die bepaalde gebruikers doorgeven of opslaan te monitoren. *Point de Contact* is sinds september 2009 ook te bereiken vanaf een mobiele telefoon.

Met betrekking tot mobiele telefonie is er nog een ander vermeldenswaardig initiatief van coregulering. De AFOM – de Franse koepelorganisatie van mobiele operators – heeft een gedragscode (*Charte d'engagements des Opérateurs sur le contenu multimedia)* met als doel om minderjarigen te beschermen tegen illegaal materiaal (zoals gedefinieerd in artikel 6-I-7, derde paragraaf LCEN, bijv. kinderporno) en gevoelig materiaal (zoals pornografisch materiaal). De gedragscode is ontwikkeld op basis van artikel 16(e) van de E-commerce richtlijn, waarin de ontwikkeling van gedragscodes wordt aangemoedigd, de Aanbeveling van de Raad om een doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken in audiovisuele en informatiediensten[144] als ook de Aanbeveling van de *Forum des droits sur l'Internet* inzake de bescherming van minderjarigen op het internet en mobiele netwerken.[145] De gedragscode is ondertekend door de leden van AFOM[146] en het Ministerie van werkgelegenheid en sociale en publieke functionarissen (*Ministère du Travail, de la Solidarité et de la Fonction Publique*). Naast de verplichtingen op grond van LCEN, zijn de mobiele operators overeengekomen om hun notificatieprocedure voor het melden van illegaal materiaal te verbeteren en dergelijk materiaal prompt te verwijderen of de toegang daartoe te blokkeren nadat zij hiervan in kennis zijn gesteld. De gedragscode is in 2006 ondertekend en vormt een onderdeel van het Europese kader van Safer Mobile Use, een Europees initiatief om te waarborgen dat kinderen en tieners via hun mobiele telefoon veilig toegang hebben tot content.

Er zijn nog twee andere initiatieven die in dit kader het vermelden waard zijn. Het eerste initiatief betreft een initiatief van het Ministerie van Binnenlandse Zaken en het tweede initiatief betreft de Aanbeveling die is gepubliceerd door het *Forum des droits sur l'Internet*.

In 2009 heeft het Ministerie van Binnenlandse Zaken een website (www.internet-signalement.gouv.fr) gelanceerd waarop internetgebruikers als ook de AFA – dankzij een specifieke toegangsconstructie via *Point de Contact* – direct melding kunnen maken van illegaal materiaal. De meldingen worden via het platform PHAROS (*Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements*), verwerkt door de politie-

---

[144] Aanbeveling van de Raad van 24 september 1998 (98/560/EC) betreffende de ontwikkeling van de concurrentiepositie van de Europese industrie van audiovisuele en informatiediensten door de bevordering van nationale kaders teneinde een vergelijkbaar en doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken, OJ L270/40, 07.10.1998.

[145] Recommandation, Les Enfants du Net (I), l'exposition des mineurs aux contenus préjudiciables sur l'Internet, 11 février 2004, Forum des droits sur l'Internet, maar ook Recommandation, Classification des contenus multimédia mobiles, 18 octobre 2006, gevestigd door een werkgroep van het *Forum,* op verzoek van AFOM nadat de Code of Conduct was vastgesteld.

[146] Bouygues Telecom, Orange France, SFR, Debitel, M6 Mobile, Universal Mobile and Omer Telecom.

eenheid die verantwoordelijk is voor cybercrime. Dit platform bestaat al enkele jaren en richtte zich oorspronkelijk enkel op de bestrijding van kinderporno.

Tot slot heeft de *Forum des droits sur l'Internet* – een onafhankelijke coreguleringsorganisatie die tot stand is gekomen met de hulp van de Franse overheid en tot doel heeft de dialoog tussen de verschillende Internetgerelateerde marktpartijen en de Franse overheid te faciliteren – drie Aanbevelingen gepubliceerd met betrekking tot het beschermen van kinderen en kinderporno. De eerste Aanbeveling[147] bestond reeds voordat de LCEN was aangenomen. In dit document doet het Forum aanbevelingen aan de publieke autoriteiten, ouders en marktpartijen. Internetserviceproviders wordt aanbevolen om informatie over kinderbescherming op hun homepage te plaatsen en de aanbieders van online materiaal wordt aanbevolen om te werken aan technische oplossingen (software) om de inhoud van online materiaal te kunnen omschrijven. De tweede Aanbeveling[148] beveelt internetserviceproviders aan om een hoge standaard ten aanzien van informatie over hun gebruikers te implementeren. Verder moedigt het Forum internetgerelateerde markt-partijen aan om een notificatiemechanisme te implementeren zoals staat omschreven in AFA's *Charte contre les contenus odieux*. De derde Aanbeveling[149] is het meest recente document van het Forum. Ten tijde van deze aanbeveling waren het Ministerie van Binnenlandse Zaken als ook het Ministerie *du Travail, de la Solidarité et de la Fonction Publique* met name geïnteresseerd in maatregelen om de toegang tot in het buitenland gesitueerde kinderpornowebsites te blokkeren. In dit verband hebben zij de werkgroep, een onderdeel van het Forum, die zich bezighoudt met kinderbescherming, gevraagd om een studie te verrichten naar de technische en juridische mogelijkheden van filteren. De derde Aanbeveling is het resultaat van het werk dat deze werkgroep heeft verricht. In dit document neemt het Forum geen standpunt in over de mogelijkheid om al dan niet filtermaatregelen op te leggen aan internetserviceproviders, maar geeft het slechts juridische en technische aanbevelingen over de manier waarop dergelijke maatregelen geïmplementeerd kunnen worden. Het Forum stelt als vooreis dat dergelijke maatregelen alleen maar van toepassing kunnen zijn op kinderporno. De voorgestelde maatregelen zien er als volgt uit. Bepaalde eenheden van de politie zouden in samenwerking met internetgebruikers (via de notificatiemogelijkheden) kinderpornografisch materiaal identificeren. Vervolgens stelt het OCLCTIC, het bureau dat verantwoordelijk is voor de bestrijding van cybercriminaliteit, een lijst van websites vast waarop beeldmateriaal of representaties van seksueel misbruik van minderjarigen wordt aangetroffen. Deze lijst wordt vervolgens door een op dit moment nog niet nader genoemde bevoegde nationale autoriteit beoordeeld en doorgezonden naar de internetserviceproviders, die de toegang tot de desbetreffende websites blokkeren, waarbij de regels van 'due process' in acht worden

[147] Recommandation, Les Enfants du Net (I), l'exposition des mineurs aux contenus préjudiciables sur l'internet, 11 février 2004, le Forum des droits sur l'Internet.

[148] Recommandation, Les Enfants du Net-II, pédo-pornographie et pédophilie sur l'internet, 25 janvier 2005, le Forum des droits sur l'Internet.

[149] Recommendation, Les Enfants du Net III, conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI, 29 octobre 2008, le Forum des droits sur l'Internet.

genomen. Internetserviceproviders zullen ofwel de lijst met websites automatisch in hun lijst met te blokkeren websites plaatsen zonder naar de desbetreffende webadressen te kijken, danwel een persoon moeten aanstellen die gelegitimeerd is om de lijst te ontvangen, te decrypteren en te verwerken alvorens de lijst in het filtermechanisme wordt ingevoerd. Internetserviceproviders zijn vrij in het kiezen van een van deze twee opties.

De door het Forum aangenomen Aanbevelingen zijn beleidsinstrumenten die normaal gesproken de overheid helpen in het ontwerpen van nieuwe wetsvoorstellen.

II. Toepassing van de regelgeving

Wettelijk kader

Internetserviceproviders en aanbieders van hostingdiensten zijn ingevolge artikel 6-I-7, vierde paragraaf LCEN, verplicht om een notificatiesysteem op te zetten die internetgebruikers in staat stelt om de aanwezigheid van illegaal materiaal, zoals kinderporno, te melden. Alle leden van AFA voeldoen aan hun wettelijke verplichting door gebruikmaking van de hierboven omschreven *Point de Contact*. Een van de grootste internetserviceproviders van Frankrijk is echter geen lid van AFA en heeft zijn eigen notificatiemechanisme opgezet.

Deze internetserviceprovider heeft op zijn website een notificatiemechanisme geïmplementeerd om materiaal zoals omschreven in artikel 6-I-7, derde paragraaf LCEN te notificeren. Internetgebruikers kunnen materiaal dat de menselijke waardigheid aantast (waaronder kinderporno) melden aan de provider door middel van het invullen van een notificatieformulier dat per post kan worden verstuurd naar de provider. Hoewel het notificatiemechanisme voldoet aan de wettelijke voorschriften, kan men zich afvragen of notificatie per post wel voldoende efficiënt is om kinderporno te kunnen bestrijden. Er zijn geen openbare cijfers bekend over het aantal ontvangen notificaties en het soort materiaal waarop de notificaties betrekking hebben.

Alle andere internetserviceproviders maken gebruik van de *Point de Contact* die is opgezet en wordt onderhouden door AFA. Ondanks het feit dat de aan de *Point de Contact* ten grondslag liggende *Charte contre les contenus odieux* juridisch niet bindend is, voldoen de ondertekenaars van dit document aan de wettelijke vereisten door op hun website door te verwijzen naar dit meldpunt. AFA onderzoekt elk jaar hoeveel notificaties er binnen komen via de *Point de Contact*. Van de 4573 websites waarvan werd gemeld dat zij kinderporno bevatten, werden er in 2009 door de analisten van het meldpunt 987 aangewezen als websites waarop mogelijk illegaal materiaal was te vinden. Deze cijfers over 2009 zijn 15% lager dan de cijfers over 2008. Volgens het persbericht[150] van AFA toont dit aan dat er een verschil zit in de waardering van het materiaal door internetgebruikers en die door de experts die het

[150] http://www.afa-france.com/p_bilan_2009_pointdecontact.html.

genotificeerde materiaal analyseren. Het lijkt erop dat de internetserviceproviders hun verplichting om illegaal materiaal te rapporteren volledig hebben gedelegeerd aan de *Point de Contact,* die in de praktijk blijkt te oordelen of het genotificeerde materiaal in strijd is met de wet of niet. Als dit het geval is dan wordt het materiaal geïdentificeerd, de handhavende autoriteit (OCLCTIC) geïnformeerd en wordt het materiaal doorgestuurd naar de aanbieder van de hostingdienst indien het materiaal wordt gehost door een aanbieder die lid is van AFA. Het materiaal wordt naar een van de internationale partners van *Point de Contact* doorgestuurd in het geval het materiaal wordt gehost door een aanbieder van hostingdiensten in het buitenland die lid is van het INHOPE netwerk. Hoewel AFA-leden via gebruikmaking van de *Point de Contact* voldoen aan hun verplichtingen van artikel 6-I-7 LCEN, ontslaat dit hen echter niet van de verplichting om materiaal dat internetgebruikers direct aan hen hebben gemeld, te rapporteren aan de handhavende autoriteiten. Op grond van de beschikbare statistieken blijkt dat maar zeer weinig internetserviceproviders de handhavende autoriteit, de OCLCTIC, direct op de hoogte brengen van vermeend illegaal materiaal. In 2007 hebben maar drie internetserviceproviders respectievelijk 2, 5 en 122 meldingen gedaan van vermeend illegaal materiaal.[151]

Overige regulering

Van de drie aangenomen Aanbevelingen van het *Forum des droits sur l'Internet* over kinderporno, is de derde Aanbeveling gebruikt door het Ministerie van Binnenlandse Zaken om een nieuw wetsvoorstel in te dienen dat internetserviceproviders verplicht tot het filteren van kinderporno.

III. Ontwikkelingen

Op 27 mei 2009 heeft het Ministerie van Binnenlandse Zaken een nieuw wetsvoorstel ingediend met de titel *Orientation et Programmation pour la Performance de la Sécurité Intérieure* (LOPPSI II).[152] Het algemene doel van deze wet is om de veiligheid van Franse burgers te verbeteren via een aantal andere doelen voor de periode 2009-2013. Cybercriminaliteit is een van de besproken onderwerpen. Hoofdstuk II van het wetsvoorstel gaat over de strijd tegen cybercriminaliteit en bevat nieuwe bepalingen om internetgebruikers te beschermen tegen kinderporno. Op grond van het voorgestelde artikel 4 van het wetsvoorstel, zal het Ministerie van Binnenlandse Zaken, onder goedkeuring van de rechterlijke macht, webadressen waarop kinderporno wordt aangeboden doorsturen naar internetservice-

[151] 'Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique', n° 627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 januari 2008, beschikbaar via: http://www.assemblee-nationale.fr/13/rap-info/i0627.asp.

[152] 'Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure', n° 1697, 27 mei, 2009, beschikbaar via: http://www.assemblee-nationale.fr/13/projets/pl1697.asp.

providers. Internetserviceproviders zijn vervolgens verplicht om deze URL's te blokkeren. Een besluit zal de verdere formaliteiten van deze procedure nader specificeren. Op dit moment is de inhoud van dit besluit onbekend en er is geen zekerheid dat dit besluit zal voorzien in een recht om te ageren tegen een onjuist besluit om een URL op een zwarte lijst te plaatsen.

De *Assemblée nationale* heeft het wetsvoorstel al besproken en aangenomen in de eerste lezing en het wetsvoorstel ligt nu bij de Sénat.[153] Wanneer het wetsvoorstel wordt besproken is nog onbekend. Er zijn wel al enkele vragen gesteld en zorgen geuit over het wetsvoorstel. Volgens de Commissie die verantwoordelijk is voor nationale veiligheid en defensie is er nog helemaal geen 'impact assessment' uitgevoerd waarin de effectiviteit van filteren als ook de globale kosten (in de zin van de compensatie voor internetserviceproviders voor de gemaakte kosten als ook de door de overheid vereiste middelen) zijn geëvalueerd. Tijdens de parlementaire behandeling in de *Assemblée nationale* zijn wel zorgen geuit over het gevaar van 'overblocking' (het filteren van materiaal dat niet gefilterd had mogen worden) en het filteren van het verkeerde materiaal, maar deze gevaren werden niet gezien als voldoende reden om het wetsvoorstel in te trekken. Er werden tevens argumenten naar voren gebracht die de effectiviteit, de proportionaliteit en de indringende aard van de voorgestelde maatregelen in twijfel trokken, maar deze argumenten werden door de meerderheid van het Franse parlement niet overtuigend geacht. Men zal verdere discussies kunnen verwachten zodra het voorstel door de Sénat wordt besproken.

[153] «Projet de loi, adopté par l'Assemblée nationale, d'orientation et de programmation pour la performance de la sécurité intérieure», n° 292, 16 februari 2010, beschikbaar via: http://www.senat.fr/leg/pjl09-292.html.

Auteursrecht

I. Wettelijk kader

Het regelgevend kader inzake het gebruik, de verveelvoudiging en distributie van auteursrechtelijk beschermde werken is te vinden in het eerste hoofdstuk van de *Code de la Propriété Intellectuelle* (CPI). De CPI is enkele malen gewijzigd. De belangrijkste wijzigingen zijn tot stand gekomen door de *Loi sur le droit d'auteur et les droits voisins dans la société de l'information*[154] (Loi DADVSI), die de Auteursrechtrichtlijn (2001/29/EC) implementeert, en door de *Loi favorisant la diffusion et la protection de la création sur Internet*[155] (Loi HADOPI), met toevoeging van enkele strafrechtelijke bepalingen door de *Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet*[156] (Loi HADOPI 2).

De CPI geeft de auteurs van literaire en artistieke werken het recht om te bepalen hoe hun werken door derden worden gebruikt. Auteursrechthebbenden hebben tevens enkele rechtsmiddelen tot hun beschikking om op te treden tegen ongeoorloofd gebruik van hun werken. Artikel L.122-4 CPI voorziet in een verbodsrecht, inhoudend dat iedere verveelvoudiging van een werk zonder toestemming van de maker of de rechthebbende onrechtmatig is. Volgens artikel L. 122-3 CPI moet men onder verveelvoudiging verstaan: iedere fysieke vastlegging van een werk die de openbaarmaking van het werk mogelijk maakt.

Alvorens de verantwoordelijkheden van internetserviceproviders te beschrijven is het van belang om een onderscheid te maken tussen de zorgplicht van internetserviceproviders die enkel toegangsdiensten verlenen en de zorgplicht van dienstenaanbieders die hostingdiensten aanbieden.

Verantwoordelijkheden van internetserviceproviders die enkel toegangsdiensten verlenen

Op grond van artikel 6-I-7 *Loi pour la confiance dans l'économie numérique* (LCEN) zijn internetserviceproviders gevrijwaard van aansprakelijkheid indien zij slechts handelen als mere conduits, zoals omschreven in de inleiding.

Indien de internetserviceprovider adverteert dat men via zijn toegangsdienst bestanden kan downloaden die hij zelf niet aanbiedt, dan moet de provider op grond van artikel 7 LCEN duidelijk in zijn advertenties aangeven dat piraterij artistieke productie ondermijnt.

---

[154] Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, JORF n° 178 du 3 août 2006, p.11529.

[155] Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n° 135 du 13 juin 2009, p.9666.

[156] Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, JORF n° 251 du 29 octobre 2009, p.18290.

Naast de verplichtingen die volgen uit de LCEN, hebben de HADOPI wetten voor internetserviceproviders extra zorgplichten in het leven geroepen. Op grond van artikel L. 336-3 CPI (artikel 335-12 CPI (oud)) moeten abonnees hun internettoegang beveiligen om online schendingen van auteursrecht te voorkomen. Ingevolge artikel 6-I-1, tweede paragraaf LCEN moeten internetserviceproviders hiertoe hun abonnees informeren over de bestaande veiligheidsmaatregelen, zodat de abonnees kunnen voldoen aan hun plicht om het gebruik van hun internettoegang te monitoren. Van de lijst van technische maatregelen opgesteld door de HADOPI autoriteit, moeten internetserviceproviders ten minste een efficiënte technische maatregel voorstellen aan hun abonnees. Op grond van artikel L. 331-27 CPI zijn de internetserviceproviders verplicht om in hun gebruikersovereenkomst de volgende elementen te vermelden: artikel L.336-3 CPI, de maatregelen die kunnen worden getroffen tegen de abonnees indien zij hun toezichtsverplichting niet nakomen, als ook de civielrechtelijke en strafrechtelijke sancties die gelden in geval van inbreuk op auteursrecht.

Naast deze informatieplicht jegens de abonnees, moeten de internetserviceproviders met de HADOPI autoriteit en de rechtbanken meewerken in zaken waarin abonnees hun toezichtsverplichting niet nakomen of inbreuk maken op het auteursrecht. Krachtens artikel L.331-25 CPI kan de *Commission de Protection des Droits*, een van de twee onderdelen van de HADOPI autoriteit, de internetserviceprovider verzoeken om een eerste waarschuwing te e-mailen naar de abonnee, indien de abonneee zich niet aan zijn toezichtsverplichting houdt. Een tweede waarschuwing volgt 6 maanden later. De rechtbank kan in het geval er sprake is van inbreuk op auteursrecht (artikel 335-7 CPI) of grove nalatigheid ten aanzien van de toezichtsverplichting (artikel 335-7-1 CPI), een extra strafmaatregel treffen inhoudende de opschorting van internettoegang voor bepaalde tijd. De HADOPI autoriteit wordt op de hoogte gesteld van de extra strafmaatregel zodra de rechterlijke beslissing uitvoerbaar is, en de strafmaatregel wordt vervolgens doorgestuurd naar de betreffende internetserviceprovider. Binnen twee weken nadat de internetserviceprovider op de hoogte is gesteld moet de internetserviceprovider de toegang tot internet van de desbetreffende abonnee blokkeren op straffe van een boete van € 5 000.

Verantwoordelijkheden van internetserviceproviders die tevens hostingdiensten verlenen

De zorgplicht van dienstenaanbieders van hostingactiviteiten (waaronder internetserviceproviders kunnen vallen) ten aanzien van op het auteursrecht inbreukmakend materiaal staat omschreven in artikel 6-I-2 en artikel 6-I-7 LCEN. Dienstenaanbieders van hostingactiviteiten hebben geen algemene plicht om de informatie die zij doorgeven en/of opslaan te monitoren. Zij hebben enkel de plicht om de informatie te verwijderen of de toegang daartoe te blokkeren indien *zij daadwerkelijk kennis hebben van de illegale aard [van de informatie of activiteit], of wanneer zij op de hoogte zijn van feiten of omstandigheden waaruit de illegale aard van de activiteit of informatie duidelijk naar voren komt.* De daadwerkelijke kennis van dienstenaanbieders van hostingactiviteiten wordt op grond van artikel 6-I-5 LCEN verondersteld, indien zij op de hoogte zijn gesteld via een notificatie die de elementen bevat op basis waarvan diegene die de informatie heeft geleverd kan worden geïdentificeerd: een omschrijving en lokalisering van de feiten, redenen voor de verwijdering en bewijs dat contact is gezocht met diegene die de informatie heeft geleverd met het verzoek deze

informatie te verwijderen. De wettelijke bepalingen die de aansprakelijkheid van aanbieders van hostingdiensten regelen moeten worden geïnterpreteerd in het licht van de beslissing van het Franse Constitutionele Hof, de *Conseil Constitutionnel,* inzake de interpretatie van de LCEN.[157] Het Constitutionele Hof hanteert in deze beslissing een strikte interpretatie van artikel 6-I-2 LCEN en oordeelt dat aanbieders van hostingdiensten alleen aansprakelijk kunnen worden gesteld voor het niet verwijderen van informatie waarvan is gemeld dat deze onrechtmatig is, indien (a) de informatie onmiskenbaar onrechtmatig is of (b) een rechtbank heeft bevolen om de informatie te verwijderen. Volgens het Constitutionele Hof hoeven aanbieders van hostingdiensten alleen te oordelen of de aard van de informatie 'onmiskenbaar onrechtmatig' is en niet of de informatie rechtmatig dan wel onrechtmatig is.

I. Toepassing van de regelgeving

Verantwoordelijkheden van internetserviceproviders die enkel toegangsdiensten verlenen

De recente HADOPI wetgeving heeft de zorgplicht afgebakend van internetservice-providers die enkel toegangsdiensten verlenen. De HADOPI autoriteit is sinds januari 2010 actief en heeft als taak om 'rechten te beschermen op het internet'. De Minister van Cultuur en Communicatie en de secretaris-generaal van de HADOPI autoriteit verwachten dat de autoriteit wegens een gebrek aan middelen niet eerder dan juli 2010 de eerste waarschuwingen per e-mail zal versturen .

Wegens een aantal technische redenen is het op dit moment niet mogelijk om de wettelijke bepalingen te handhaven. De hierboven vermelde lijst van veiligheidsmaatregelen die de HADOPI autoriteit moet opstellen, bestaat momenteel nog niet. Daarnaast is het besluit (zoals voorzien door artikel 331-26 CPI) waarin wordt uiteengezet hoe de veiligheidsmaatregelen moeten worden beoordeeld en hoe zij moeten worden voorzien van een kwaliteitslabel nog niet aangenomen. Daarenboven moet de overheid nog steeds een definitie geven van wat exact te verstaan is onder 'grove nalatigheid' van de abonnee die zijn toezichtsverplichting niet nakomt.[158]

Verantwoordelijkheden van internetserviceproviders die tevens hostingdiensten verlenen

De verantwoordelijkheden voor aanbieders van hostingdiensten wordt geregeld in artikel 6-I-2 e.v. LCEN. De exacte reikwijdte hangt af van de interpretatie. Het Constitutionele Hof besliste in de hierboven aangehaalde beslissing (2004-496 DC) dat artikel 6-I-2 LCEN zodanig geïnterpreteerd moet worden dat aanbieders van hostingdiensten bij het ontbreken van een rechterlijk bevel alleen dan materiaal dienen te verwijderen dat onmiskenbaar onrechtmatig is. Het begrip 'onmiskenbaar onrechtmatig' is niet gedefinieerd, maar sommige commentatoren zijn van oordeel dat de lijst van zeer schadelijk en onrechtmatig

[157] Décision n° 2004-496 DC, JORF du 22 juin 2004, p. 11182.

[158] Eind juni 2010 wordt een besluit hieromtrent verwacht, maar er is nog geen officiële informatie bekend over de inhoud van dit besluit.

materiaal zoals omschreven in artikel 6-I-7, paragraaf 3 LCEN (o.a. informatie inzake misdrijven tegen de menselijkheid, rassenhaat, kinderporno, tot geweld aanzettende of de menselijke waardigheid aantastende informatie) onder de reikwijdte van dit begrip valt.

Er is echter nog nooit een verband gelegd tussen de interpretatie van het Constitutionele Hof en de lijst van illegaal materiaal zoals omschreven in artikel 6-I-7, paragraaf 3 LCEN.[159] Sommige rechtbanken hebben het begrip onmiskenbaar onrechtmatig opgerekt tot andere informatie.[160] Ten aanzien van op het auteursrecht inbreukmakend materiaal hebben de rechtbanken geoordeeld dat dit niet onmiskenbaar onrechtmatig is.[161]

De aanbieders van hostingdiensten zijn echter wel verplicht om het inbreukmakend materiaal te verwijderen zodra zij via de notificatieprocedure van artikel 6-I-5 LCEN in kennis zijn gesteld. Hoewel deze notificatieprocedure vrijblijvend is, lijken de rechtbanken de procedure als een verplichting te zien bij de beoordeling of de aanbieder van hostingdiensten daadwerkelijk kennis heeft van de aanwezigheid op zijn website van inbreukmakend materiaal. Zodra de aanbieder op de juiste wijze in kennis is gesteld (bijvoorbeeld via de notificatieprocedure) is het verplicht om het materiaal te verwijderen. In dit verband is het vermeldenswaardig dat zowel het gerecht van eerste aanleg (*Tribunal de Grande Instance)* als ook de Parijse hoger beroep rechter (*Cour d'appel de Paris)* hebben geoordeeld dat de aanbieder van hostingdiensten niet aansprakelijk kan worden gesteld voor het niet verwijderen van vermeend inbreukmakend materiaal, bij afwezigheid van een volledig correcte notificatie (o.a. het ontbreken van de desbetreffende URL, de titels of de locatie van vermeend inbreukmakend materiaal).[162]

Lagere rechtbanken hebben tevens een nieuwe verantwoordelijkheid gecreëerd die aanbieders van hostingdiensten verplicht tot het voorafgaand monitoren van opvolgende inbreukmakende handelingen met reeds geïdentificeerd inbreukmakend materiaal. Volgens de *Tribunal de Grande Instance de Paris*, heeft de aanbieder van hostingdiensten de plicht om verdere publicatie van inbreukmakend materiaal door andere internetgebruikers te voorkomen zonder voorafgaande notificatie, zodra de aanbieder dit materiaal naar aanleiding van een eerdere notificatie reeds heeft verwijderd.[163] Dezelfde rechtbank heeft in

---

[159] Thoumyre (2008).

[160] CA Paris, 14ème ch.A, 12 december 2007, Google Inc et Google France v. Benetton Group et Bencom (inbreuk op merkrecht en onrechtmatig materiaal).

[161] TGI Paris, 15 april 2008, Jean-Yves Lafesse v. Dailymotion ; TGI Paris 15 april 2008, Omar & Fred v. Dailymotion ; TGI Paris, 22 september 2009, ADAMI, Omar & Fred v. YouTube.

[162] TGI Paris, 24 juni 2009, Jean-Yves Lafesse v. Google ; CA Paris, 6 mei 2009, Dailymotion v. Nord Puest Productions & UGC Images.

[163] TGI de Paris, Zadig Productions v. Google Video, 19 oktober 2007; TGI de Paris, Ordonnance de référé, Roland Madgane et autres v. YouTube, 5 maart 2009; TGI Paris, 10 april 2009, Zadig Productions v. Dailymotion.

een andere zaak zijn positie ten aanzien van deze problematiek iets gewijzigd in een zaak waarin de aanbieder van hostingdiensten het voorstel deed om een watermerk toe te voegen aan het materiaal. Met behulp van software zou het dan mogelijk zijn om in kennis te worden gesteld van nieuw inbreukmakend materiaal. De eisende partij in deze zaak reageerde hierop echter niet. Onder deze omstandigheden was de rechtbank van oordeel dat de aanbieder van hostingdiensten niet aansprakelijk kan worden gehouden voor iedere keer dat het reeds genotificeerde inbreukmakende materiaal beschikbaar wordt gesteld op de server van de aanbieder. [164]

[164] TGI Paris, 24 juni 2009, Jean-Yves Lafesse v. Google Video.

Identiteitsfraude

I. Huidige regelgeving

Wettelijk kader

De relevante Franse wettelijke bepalingen ten aanzien van identiteitsfraude kan men vinden in de artikelen 433-19, 434-23 en 313-1 van de *Code pénal* (het Franse wetboek van strafrecht) en in artikel 781 van de *Code de procédure pénale* (het Franse wetboek van strafvordering).

Het gebruik van een ander zijn naam of een gedeelte daarvan als ook de wijziging of aanpassing van de naam van een ander in een authentiek document of een administratief document opgemaakt voor een publieke autoriteit is op grond van artikel 433-19 *Code pénal* strafbaar. Hierop staat een gevangenisstraf van 6 jaar en een boete van € 7.500. Op grond van artikel 781 van de *Code de procédure pénale* is het strafbaar om gebruik te maken van een valse naam om het strafblad van een ander te verkrijgen.

Volgens artikel 434-23 van de *Code pénal*, is het gebruik van de naam van een ander alleen dan strafbaar als de naam wordt gebruikt in zodanige omstandigheden dat dit ertoe leidt of zou leiden dat de persoon wiens identiteit is gestolen strafrechtelijk wordt vervolgd. Hierop staat een gevangenisstraf van 5 jaar of een boete van € 75.000. Onder Frans recht is dus het enkele gebruik van de naam van een ander niet strafbaar. Alleen de consequenties van de identiteitsdiefstal (zoals het plegen van fraude onder een valse naam ex artikel 313-1 van de *Code pénal)* en niet de identiteitsdiefstal zelf zijn strafbaar.

Internetserviceproviders hebben geen formele verantwoordelijkheid met betrekking tot het voorkomen, bestrijden of opsporen van identiteitsfraude. Zij hebben enkel de plicht om op grond van artikel 34 van *Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* (Loi Informatique et Libertés) een inbreuk op persoonsgegevens – hetgeen zou kunnen leiden tot identiteitsfraude – te voorkomen. Op grond van dit artikel zijn de voor de verwerking verantwoordelijke natuurlijke personen en rechtspersonen (waaronder internetserviceproviders) verplicht om alle nodige voorzorgsmaatregelen te treffen, rekening houdend met de aard van de persoonsgegevens en de risico's van de verwerking, om de veiligheid van deze persoonsgegevens te waarborgen en in het bijzonder om te voorkomen dat de persoonsgegevens worden gewijzigd, beschadigd of ongeautoriseerde derden hiertoe toegang hebben (zie ook de paragraaf over internetveiligheid).

Overige regulering

In 2006 werd het Directoraat dat verantwoordelijk is voor de ontwikkeling van de media (een dienst van de minister-president), gevraagd om publieke aandacht te genereren voor de veiligheid van transacties op het internet. Het doel was om het gebruik van hulpmiddelen waarmee men zich kan authentificeren te vergroten om zodoende identiteitsfraude te voorkomen. Volgens de staatssecretaris die verantwoordelijk is voor strategische studies en de ontwikkeling van de digitale economie[165], Nathalie Kosciusko-Morizet, staat identificatie toe dat de identiteit wordt geopenbaard, terwijl authentificatie garandeert dat de gesprekspartner van de gebruiker daadwerkelijke degene is die hij pretendeert te zijn. Authentificatie wordt gedefinieerd als een manier waarop wordt voorkomen dat persoonsgegevens in geval van fraude worden gebruikt om een transactie te ondertekenen met een gestolen identiteit. De discussie met en de consultatie van professionals en publieke autoriteiten heeft geleid tot de ondertekening van een *Charte pour la promotion de l'authentification sur Internet* (Charter ter promotie van authentificatie op het internet). Het charter werd voor het eerst door de publieke autoriteiten ondertekend in februari 2008, en in juni 2009 door de marktpartijen – onder andere Free, eBay en Yahoo!France. Het charter bevat geen artikelen, maar principes waaraan de ondertekende partijen zich binden: de informatievoorziening aan gebruikers met betrekking tot kwaadaardig gedrag (zoals spam, *phishing*) maar ook de bevordering van gepaste authentificatie gebruiken en authentificatie methoden om computers te beveiligen. Op 1 februari 2010 heeft de staatssecretaris, die de leiding heeft over de strategische studie en de ontwikkeling van de digitale economie, een nieuw kwaliteitsstempel geïntroduceerd met naam 'IDéNum', een enkel elektronisch identiteitscertificaat om wachtwoorden en gebruikersnamen voor publieke en private websites te vervangen door een klein beveiligingsapparaat. De Franse Federatie van Banken (FBF) en de Franse Federatie van Verzekeringsmaatschappijen (FFSA) behoren tot de partners.[166]

II. Toepassing bestaande regelgeving

Wettelijk kader

Met betrekking tot de definitie en de vervolging van identiteitsfraude (onder artikel 434-23 van de C*ode pénal*), heeft het Franse cassatiehof beslist dat identiteitsfraude alleen strafbaar is wanneer het delict waarbij de identiteit is gestolen ook zelf strafbaar is. Wanneer het delict van identiteitsfraude samenhangt met lasterlijke activiteiten, die niet bewezen kunnen

[165] "Nathalie-Kosciusko-Morizet mobilizes actors of the digital environment to increase the Internet users' security", Press Release relating to the signature of the "Charter to promote authentification on the Internet", 17 June 2009.

[166] "Présentation du Label IDéNum, l'identité numérique multi-services », Press Release, 01 February 2010, beschikbaar op: http://www.telecom.gouv.fr/fonds_documentaire/internet/presentation_IDeNum.pdf.

worden of nietig zijn, dan is identiteitsfraude niet strafbaar.[167] De opzet bij het frauderen met een gestolen identiteit is van cruciaal belang. Als het gebruik andermans elektronische adres geen identiteitsfraude oplevert, dan is het elektronische adres een online identiteit. [168]

Overige regulering

Het *Charte pour la promotion de l'authentification sur Internet* is ondertekend door verschillende web 2.0 platforms, maar slechts door één internetserviceprovider: Free. Het moet worden opgemerkt dat de AFA, de Franse organisatie die de belangen van internetserviceproviders vertegenwoordigt, het document niet heeft ondertekend ondanks dat het raakt aan de activiteit van zijn leden.

III. Ontwikkelingen

In Frankrijk is sinds enkele jaren het probleem van identiteitsfraude als prioriteit aangemerkt.[169] In 2005[170] en 2008[171] hebben twee senatoren een wet voorgesteld die identiteitsfraude zonder frauduleuze bedoelingen criminaliseert. Geen van deze voorstellen is ooit in het parlement besproken.

Het Franse Minsterie van Binnenlandse zaken heeft echter ook op 27 mei 2009 een wet op de *Orientation et Programmation pour la Performance de la Sécurité Intérieure* (LOPPSI II, Oriëntatie en Programmeren voor Interne Veiligheid) voorgesteld.[172] Het doel van het wetsvoorstel is om de veiligheid van Franse burgers, door doelen die zijn opgesteld voor 2009 tot 2013, te verbeteren. Computercriminaliteit is één van de onderwerpen die worden aangepakt. Hoofdstuk II van het voorstel heeft betrekking op de bestrijding van computercriminaliteit

[167] Cour de Cassation, Chambre Criminelle, N. 05-85857, 29 Mars 2006; Cour de Cassation, Chambre Criminelle, N. 06-84365, 30 Mai 2007 linked to Cour de Cassation, Chambre Criminelle, N.08-83255, 20 Janvier 2009.

[168] Cour de Cassation, Chambre Criminelle, N.08-83255, 20 Janvier 2009.

[169] In 2005 werd ook een project van online ID (CNIE-Carte d'Identité Numérique) gestart.

[170]'Proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques', n° 452, by M. Michel Dreyfus-Schmidt, 4 July 2004, beschikbaar op: http://www.senat.fr/leg/ppl04-452.html.

[171] 'Proposition de loi relative à la pénalisation de l'usurpation d'identité numérique', n° 86, by Mme Jacqueline Panis, 6 November 2008, beschikbaar op: http://www.senat.fr/leg/ppl08-086.html.

[172] 'Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure', n° 1697, 27 May , 2009, beschikbaar ophttp://www.assemblee-nationale.fr /13/projets/ pl1697.asp.

en introduceert een nieuw artikel 222-16-1 in de C*ode pénal*, dat twee nieuwe delicten met betrekking tot identiteitsfraude introduceert. Het gebruik maken van een identiteit van een derde partij of data ter identificatie op een elektronisch netwerk is strafbaar wanneer er opzet is om de rust te verstoren *('tranquilité*) of de eer of goede naam te beïnvloeden. Beide delicten zullen worden gestraft met 1 jaar gevangenisstraf en een boete van 15.000 euro. Het voorstel is al aangenomen door het Franse parlement[173] en is ter bespreking en aanname doorgestuurd naar de Franse senaat. Tijdens de bespreking van het voorstel zijn verschillende opmerkingen gemaakt met betrekking tot de proportionaliteit van de zin en de vage notie van 'het verstoren van iemands rust'.

[173] 'Projet de loi, adopté par l'Assemblée nationale, d'orientation et de programmation pour la performance de la sécurité intérieure', n° 292, 16 February 2010, beschikbaar op: http://www.senat.fr/leg/pjl09-292.html.

Verkoop gestolen goeden

I. Bestaande regelgeving

Wettelijk kader

De regels met betrekking tot de verkoop van gestolen goederen kunnen worden gevonden in artikel L. 321-3 van de Franse *Code de commerce* (Wetboek van Handelsrecht) en in artikel 311-1 en volgende van het Franse C*ode pénal* (Wetboek van Strafrecht).

Veilingwebsites zijn gedefinieerd in artikel L.321-3 van de *Code de commerce*, waarin een onderscheid wordt gemaakt tussen echte online veilingen, waarbij een derde partij een product verkoopt aan de hoogste bieder, tot aan courtage bij online veilingen, die worden gekenmerkt door het aanbrengen van de verkoop via een veiling en de interventie van een derde partij. Deze laatstgenoemde vorm wordt niet als een publieke veiling aangemerkt in de zin van artikel L 321-3 en is alleen onderworpen aan deze wet wanneer ze betrekking heeft op cultureel eigendom.

Met betrekking tot de verkoop van gestolen goederen bepaalt artikel 311-1 van de *Code pénal* dat het frauduleus verkrijgen van goederen die toebehoren aan iemand anders wordt gestraft met een gevangenisstraf van 3 jaar en een boete van 45.000 euro. Het verkrijgen van gestolen goederen of het overdragen van goederen die langs misdadige weg zijn verkregen, of het bijdragen daaraan, wordt gestraft met 5 jaar gevangenisstraf en een boete van 375.000 euro (artikel 321-2 van de *Code pénal)*.

Er zijn geen bepalingen die de verantwoordelijkheid van tussenpersonen regelt wanneer het gaat om gestolen goederen op veilingwebsites. Op grond van artikel 6 LCEN, dat artikel 15 van de E-commerce richtlijn implementeert, hebben tussenpersonen geen algemene verplichting om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden. Hosting providers hebben slechts de verplichting om onrechtmatige inhoud te verwijderen wanneer zij daarvan op de hoogte zijn gesteld of wanneer zij daarvan op de hoogte hadden moeten zijn (zoals beschreven in de inleiding).

Overige regulering

Met betrekking tot de verkoop van gestolen goederen op veilingwebsites kan slechts één initiatief genoemd worden. Het *Forum des droits sur l'Internet*, een co-regulerend en onafhankelijk orgaan, heeft een aanbeveling gedaan met betrekking tot de specifieke

aspecten van het online veilen van culturele goederen. Een deel is gewijd aan het handelen in gestolen culturele goederen.[174] Geïnspireerd door de regels die van toepassing zijn op 'offline' veilingen, heeft het Forum voorgesteld om een register bij te houden van culturele goederen en een beschrijving daarvan die online te koop staan om de verkopers van de goederen te kunnen identificeren (een aanpassing van het huidige artikel 321-7 van de *Code pénal*). De gegevens worden gedurende een periode van maximaal vijf jaar bewaard. Het Forum beveelt ook aan om voor de verkoop een online advertentie te plaatsen en ook de samenwerking tussen online makelaars en de publieke autoriteiten te versterken door het gebruik van technologische hulpmiddelen, zoals een register met beschrijvingen van gestolen goederen. De aanbeveling creëert voor tussenpersonen geen specifieke zorgplichten met betrekking to de handel in gestolen culturele goederen.

In dit deel kan ook een ander initiatief met betrekking tot de verkoop van gestolen goederen op veilingwebsites worden vermeld. In 2009 vroeg de overheid aan experts[175] om een protocol vast te stellen voor de samenwerking tussen e-commerce platforms (veilingwebsites) en merkrechthebbenden met betrekking tot de verkoop van namaakproducten. In december 2009 werd een *Charte pour lutter contre la contrefaçon sur internet* (Charter ter bestrijding van online namaakproducten) ondertekend door merkrechthebbenden en de e-commerce platforms.[176] Het document bevat *best practices* die zijn opgesteld in 17 artikelen die omstandigheden beschrijven waarin door samenwerking de verkoop van namaakproducten bestreden kunnen worden. De partijen hebben zich ertoe verbonden om gedurende 18 maanden te werken aan concrete oplossingen. De e-commerce platforms hebben ingestemd met het implementeren van technologische maatregelen om namaakproducten en verkopers daarvan op te sporen. Het Charter creëert een notice and takedown-systeem waar merkhouders de e-commerce platforms op de hoogte kunnen stellen van de verkoop van namaak producten, waarna de platforms deze aanbiedingen zullen verwijderen en de verkopers zullen bestraffen (opschorting en verwijdering van hun accounts) en zullen voorkomen dat de verkopers zich opnieuw aanmelden. Het Charter biedt ook regels met betrekking tot het opsporen van verkopers die mogelijk namaakproducten verkopen in de Europese Economische Ruimte.

Door het gebrek aan specifieke juridische verplichtingen hebben sommige veilingwebsites eigen interne regels opgesteld waaraan verkopers moeten voldoen willen zij hun producten te koop aan kunnen bieden. Gestolen goederen mogen niet te koop worden aangeboden. eBay France herinnert gebruikers op zijn website aan de strafrechtelijke bepalingen die van toepassing zijn op de verkoop en het verkrijgen van gestolen goederen.[177] eBay heeft bovendien specifieke regels vastgesteld omtrent de verkoop van gestolen goederen en heeft

[174] Recommandation, le courtage en ligne des biens culturels, juillet 2004, le Forum des droits sur l'Internet.

[175] Bernard Brochand, Voorzitter van het Nationale Comité tegen namaakproducten (CNAC) en Pierre Sirinelli, Professor aan de Universiteit van Parijs 1 (Panthéon-Sorbonne) en lid van de Hoge Raad van Literair en Artistiek Eigendom (CSPLA).

[176] http://www.economie.gouv.fr/actus/091216charte-internet.html.

[177] http://pages.ebay.fr/help/classifieds/policies-stolen.html.

het VeRO (P*rogramme d'aide à la protection de la propriété intellectuelle*- Verified Rights Owners) systeem geïntroduceerd. In dit programma kunnen rechthebbenden aan eBay doorgeven dat bepaalde goederen inbreuk maken op hun intellectuele eigendomsrechten. Aangebrachte inhoud wordt door een speciaal eBay-team afgehandeld.

II. Toepassing bestaande regelgeving

Wettelijk kader

Met betrekking tot de aansprakelijkheid van tussenpersonen voor de verkoop van gestolen goederen, speelt de status van veilingwebsites de belangrijkste rol. Verschillende rechters, zoals de *Cour d'appel de Paris* (Franse hoger beroep rechter), hebben bepaald dat eBay dient te worden aangemerkt als hosting provider zoals is geregeld in 6-I-2 van de LCEN en zij niet verantwoordelijk is voor het doen van onderzoek naar 'de kwaliteit, veiligheid en rechtmatigheid van de voorgestelde producten als ook de waarheid en correctheid van advertenties die online zijn geplaatst, de hoedanigheid van de verkopers om producten en services te verkopen, en de hoedanigheid van de kopers om te betalen voor de producten en services'.[178]

Deze uitspraak werd door de *Cour de Cassation* (Franse cassatierechter) bevestigd, maar dit Hof hoefde niet te beslissen over de status van eBay.[179] Het moet opgemerkt worden dat het *Tribunal de commerce* (Gerecht van Eerste Aanleg in het Handelsrecht), in drie beslissingen van 30 juni 2008, een andere trend heeft ontwikkeld. In zaken die betrekking hebben op de verkoop van namaakproducten, weigert het Gerecht van Eerste Aanleg om eBay te kwalificeren als hosting provider omdat het gaat om een commercieel platform dat als tussenpersoon tussen verkopers en kopers fungeert en niet slechts als een hosting provider. Artikel 6-I-2 LCEN was niet van toepassing op eBay wiens aansprakelijkheid was gebaseerd op artikelen 1382 en 1383 van het Burgerlijk Wetboek. Als een makelaar had eBay de verplichting om zich te onthouden van het faciliteren van onrechtmatig handelen zoals het verkopen van namaakproducten. eBay werd aansprakelijk gehouden voor het gebrek aan toezicht en het nalaten van het nemen van efficiënte en geschikte maatregelen tegen de verkoop van namaakproducten.

De status van e-commerce platforms is ook in twee rapporten aan de orde gekomen. Het rapport over de toepassing van de Wet op Vertrouwen in de Digitale Omgeving[180] pleit

---

[178] Cour d'Appel, Paris, 14e chambre, Section B, eBay v. DWC, 9 Novembre 2007 ; TGI Strasbourg, 1ère chambre civile, Jean L. v. eBay France, 15 Décembre 2009.

[179] Cour de Cassation, Chambre commerciale, DWC v. eBay, 5 Mai 2009.

[180] « Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » nº 627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 January 2008, beschikbaar op http://www.assemblee-nationale.fr/13/rap-info/i0627.asp.

voor een aanpassing van de aansprakelijkheid van hosting providers voor web 2.0 platforms. In het bijzonder met betrekking tot eBay en andere veilingwebsites suggereert het rapport een nieuwe status van website manager die wel aansprakelijk gehouden kan worden voor het creëren van een mechanisme ter bestrijding van namaakproducten, maar niet voor het daadwerkelijke verkopen van namaakproducten. Het rapport over tussenpersonen door het *Conseil supérieur de la propriété littéraire et artistique* (CSPLA, Hoge Raad voor Literaire en Artistieke Eigendom) bespreekt de status van commerciële platforms en concludeert dat het toepasselijke aansprakelijkheidsregime afhankelijk moet zijn van het type activiteit dat door het platform word ondernomen en niet de door het platform gegeven kwalificatie.[181] Een e-commerce platform zou daarom aansprakelijk gehouden kunnen worden onder het hosting provider aansprakelijkheidsregime voor het hosten van inhoud en onder het civielrechtelijke aansprakelijkheidsregime voor andere activiteiten, zoals makelaardij.

Overige regulering

Voor zover onze kennis strekt heeft de aanbeveling van het *Forum des droits sur l'Internet* geen wetswijzigingen tot gevolg gehad. Het moet daarbij ook opgemerkt worden dat de aanbeveling slechts van toepassing is op de online handel van culturele goederen.

Met betrekking tot het *Charte pour lutter contre la contrefaçon sur Internet* geldt dat het document door slechts twee Franse e-commerce platforms is ondertekend: PriceMinister and 2xmoinscher. Omdat Amazon en eBay hebben geweigerd het document te ondertekenen, heeft het slechts beperkte betekenis.

[181] Rapport, Commission spécialisée sur les prestataires de l'internet, Conseil supérieur de la propriété littéraire et artistique, 21 juin 2008, www.cspla.culture.gouv.fr.

2. Begeleidingscommissie

De heer prof. mr. F.W. Grosheide (voorzitter)
Universiteit Utrecht - Molengraaff Instituut voor Privaatrecht

De heer dr. F.W. Beijaard
Ministerie van Justitie - Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

De heer prof. dr. M.J.G. van Eeten
Technische Universiteit Delft - Faculteit der Techniek, Bestuur en Management (TBM)

Mevrouw dr. M. van der Linden
Universiteit Utrecht - Faculteit der Rechtsgeleerdheid

De heer ing. R. Volf
Ministerie van Economische Zaken - Directoraat-generaal Energie en Telecom

De heer drs. ing. G.J.C. Wabeke
KPN

Mevrouw A.H.G. van Zantvoort
Ministerie van Justitie - Directie Rechtshandhaving en Criminaliteitsbestrijding

3. Interviews

Nederland

Organisatie	Personen	Functie
Bits of Freedom	Ot van Daalen	Directeur
eBay.nl	Stefan Krawczyk	Senior Director and Counsel Government Relations Europe
Google	Sarah Greenwood	European Policy Manager
Google Netherlands	Jeroen Schouten	Legal counsel Benelux
ISP Connect	Arnout Veenman	Voorzitter
KPN Security	Gert Wabeke	Manager 'Justitieel' Aftappen en Monitoren
Marktplaats.nl	Foekje Croles	Head of Legal European Classifieds
Marktplaats.nl / eBay.nl	Chantal Malfeyt	Trust & Safety Manager
Ministerie van Economische Zaken	Roman Volf	Directoraat-generaal Energie en Telecom
Ministerie van Justitie	Erik Planken	Senior beleidsadviseur
Ministerie van Justitie	Anja van Zantvoort	Directie Rechtshandhaving en Criminaliteitsbestrijding

Organisatie	Personen	Functie
OPTA	Daan Molenaar	Plaatsvervangend Afdelingshoofd Consument, Nummers en Bestuur
Politie Limburg-Zuid	Peter Reijnders	Nationaal programma manager kinderpornografie
Vrije Universiteit (VU)	Rik Kaspersen	Hoogleraar
XS4ALL	Margreth Verhulst	Public Affairs & Regelgeving

Verenigd Koninkrijk

Organisatie	Personen	Functie
ISPA UK	Andrew Kernahan	Policy Officer
Ministry for Business, Innovation and Skills	Nigel Hickson	Head of Global ICT Policy
OFCOM	Jeremy Olivier	Head of Multimedia
Queen Mary University/ IWF	Ian Walden	Professor of Information and Communications Law / IWF Independent Vice-Chair
SOCA e-crime unit	Jonathan Flaherty	Technical Senior Officer
	Richard Hyams	Technical Senior Officer
Vodafone	Neil Brown	Legal Advisor
	Stephen Deadman	Executive Solicitor and Vodafone's Group Privacy Officer
	Richard Feasey	Public Policy Director

Duitsland

Organisatie	Personen	Functie
Bundesministerium für Wirtschaft und Technologie + Bundesministerium für Justiz	Rolf Bender	Department VI B 4 – Medienrecht und Neue Dienste
	Marcus Schladebach	Department für Telecommunications Recht
BITKOM – Bundesverband Informationswirtschaft	Guido Brinkel	Bereichsleiter Telekommunikations- und Medienpolitik
FSM – Freiwillige Selbstkontrolle Multimedia-Dienstanbieter	Sabine Frank	Managing director
eco – Verband der deutschen Internetwirtschaft	Frank Ackermann	Director Self-Regulation eco; Vice President INHOPE
Deutsche Telekom AG	Veronica Frey	Senior Manager Media Regulation
	Andreas Goeckel	Leiter Multimedia- und Internetrecht

Frankrijk

Organisatie	Personen	Functie
Ministère de l'Enseignement supérieur et de la recherche	Bernard Benhamou	Délégué aux Usages de l'internet
ARCEP (l'Autorité de Régulation des Communications Electroniques et des Postes)	Loïc Taillanter	Directeur juridique adjoint
	Joëlle Toledano	Membre
CNIL (Commission Nationale de l'Informatique et des Libertés)	Gwendal Le Grand	Chef du Service de l'Expertise Informatique
	Leslie Bass	Juriste
OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)	Adeline Champagnat	Commissaire de police
AFA (Association des Fournisseurs d'Accès et de Services Internet)	Quentin Aoustin	Juriste - analyste de contenus
AFA	Nicolas d'Arcy	Juriste - analyste de contenus
Free	Alexandre Archambault	Legal Advisor
	Nicolas Jaeger	Public Relations
Centre National de la Recherche Scientifique (CNRS)	Pierre-Jean Benghozi	Directeur de recherche
Forum des droits sur l'Internet	Laurent Baup	Juriste – Chargé de mission
	Stéphane Grégoire	Juriste – Chargé de mission

Summary

Commissioned by the WODC (Wetenschappelijk Onderzoek- en Documentatiecentrum), research has been conducted on duties of care on the Internet, more specifically from the perspective of Internet service providers. Internet service providers currently find themselves in the spotlight, both in a national and international context, with regard to their relationship both with governments and other private parties, on for example questions of (civil) liability. This research focuses on duties of care as concerns the relationship between government and Internet service providers. When such a duty of care does not exist, whether or not duties of care have been developed for others along the value chain between providers of information services and end-users, including Internet service providers, was examined.

The situation in four countries – the Netherlands, the UK, Germany and France – was researched. The (self-) regulation with respect to five separate themes (Internet security and safety, child pornography, copyright, identity fraud and the trade in stolen goods through Internet platforms) was identified. In addition to this, a significant number of interviews with stakeholders were conducted.

The research presents divergent results, which indicates that the related issues are still in a developing stage. Internet security and safety, more specifically the relationship between the Internet service provider and the end-user, has only been dealt with in a preliminary manner. This does not mean that in practice nothing happens, but there is a lack of formal embedding in regulation or self-regulation. With respect to child pornography, an almost identical regime exists in the examined countries. Stakeholders offer far-reaching cooperation in the fight against child pornography. All countries have established a system of hotlines for the notification of child pornography, based on self-regulation or a duty of care defined by legislation. A recurring subject of debate in the context of the fight against the dissemination of child pornography is the applicability of filtering and blocking measures. Copyright attracts a lot of attention, which has led to more stringent regulation of copyright issues in two of the examined countries, providing the possibility of cutting or limiting the access of end-users to the Internet. There is a lot of criticism on these more stringent regulations and, through the conducted interviews, stakeholders have raised clear concerns on the effective enforceability of the new rules. When dealing with identity fraud, the measures are focused on its consequences. There is not a lot of support for criminalizing identity fraud as such (in addition to already existing possibilities to counter identity fraud through other public laws). The sale of stolen goods through platform providers (i.e. auction and trading websites) is considered to be the responsibility of these providers.

The divergent results, which are proof of an ongoing dynamic in these fields and an ongoing search to find a right balance, imply that it is not possible to present proven best

practices. This also implies that on the one hand there is still a lot of insecurity, while on the other a clear challenge is presented for further policy-making. Nevertheless, the collected research results provide interesting information.

The authors present the following conclusions based on the conducted research:

1. Towards a value-chain approach

The examined duties of care cannot be related to one specific party in the value chain between information service providers and end-users. They should be considered as a shared – and balanced – responsibility of all involved stakeholders in the value chain of which, in addition to Internet service providers, providers of information services, platforms, search engines and hosting services are part.

2. Ex ante examination of effectiveness and enforceability

Examination in advance of the effectiveness and enforceability of (planned) legal intervention can contribute to the prevention of symbolic legislation and undesired effects.

3. Usability of "notice and take down" procedures

"Notice and take down" procedures are a widely accepted and applied mechanism. Not only do Internet service providers apply these or similar procedures (when acting as a provider of hosting or caching services), but other parties in the value chain, such as platform providers, do the same. In most of the examined countries, a specific legal ground for this practice is missing. Self- and co-regulatory initiatives exist however. It is recommended to further embed "notice and take down" procedures, for example by implementing a specific legal framework.

4. Clarification of Internet security, safety and privacy

The new provisions on Internet security, safety and privacy (more specifically, Article 4 of the European Directive on privacy and electronic communications) are unclear and demand further clarification on their meaning and impact. Clarification at the European level is desirable to prevent excessive divergences at the national level.

5. Elevation of the knowledge level

The inclination to develop and apply further regulation is partly caused by a lack of sufficient technical and practical knowledge. This lack of knowledge appears to be widespread. It is to be expected that the inclination to regulate will decrease when end-users, regulatory authorities, enforcement authorities and legislators will increase their knowledge level. The importance of education is widely emphasised.