

Nr. 23 De Leon & Vivi Down/Google

Op 24 februari 2010 komt de rechtbank te Milaan tot het oordeel dat drie werknemers van Google Italië, dat eigenaar is van YouTube, aansprakelijk zijn voor materiaal dat door een gebruiker op YouTube is geplaatst, te weten een video waarin is te zien hoe een autistisch kind wordt gepest.¹ De aanklacht luidt enerzijds laster anderzijds schending van de privacy. De rechter spreekt de vier gedaagden vrij van laster en veroordeelt drie van hen tot zes maanden voorwaardelijke gevangenisstraf voor schending van de privacy.

1. Partijen

Aanklager: De staat wordt vertegenwoordigd door de openbaar aanklager te Milaan.

Gedaagden:

- (1) David Carl Drummond: president van de raad van bestuur van Google Italië.
- (2) George Reyes: lid van de raad van bestuur van Google Italië.
- (3) Peter Fleischer: hoofdverantwoordelijke voor het privacybeleid van Google in Europa.
- (4) Arvind Desikan: verantwoordelijk voor Google Video's in Europa. Deskian wordt slechts laster ten laste gelegd.

Gevoegden (in Italië bestaat de mogelijkheid voor partijen om zich ter verkrijging van een schadevergoeding te voegen in een strafzaak):

- (1) De Leon: De vader van het autistisch kind. Hij heeft zich tijdens het proces teruggetrokken.
- (2) Vivi Down: organisatie die opkomt voor de belangen van kinderen met het Syndroom van Down.

Overige rechtszaken:

- (1) De groep scholieren die het kind hebben gepest, de video hebben gemaakt en de video hebben geplaatst op YouTube zijn mede op basis van de gegevens die zijn verstrekt door Google geïdentificeerd en veroordeeld door een rechtbank in Turijn tot een werkstraf oplopend tot 1 jaar.
- (2) Tegen de leraar van de school in Turijn waaraan de kinderen hun onderwijs genoten is aangeklaagd voor nalatigheid en onzorgvuldig gedrag. Deze rechtszaak is thans onder de rechter.

2. Feiten

Op 24 maart 2006 wordt er een video gemaakt in Turijn. Deze video wordt geupload op een tijdstip tussen 8 en 10 september. Dit wordt gedaan door Julia Lisa, die geen partij is bij deze strafzaak. Op de video is te zien hoe een autistische jongen wordt vernederd en fysiek wordt bedreigd door een groep jongeren uit Turijn. Het filmpje duurt een aantal minuten. Na anderhalve minuut verschijnt er een tekst, met een beledigend karakter ten aanzien van mensen met het Syndroom van Down, onder de naam van Vivi Down. Hiermee wordt de suggestie gewekt dat de organisatie deze video heeft geplaatst of haar plaatsing heeft goedgekeurd, terwijl geen van beide het geval is.

De video staat twee maanden op YouTube en is toegankelijk voor iedereen. De video wordt in totaal 5500 keer bekeken en wordt opgenomen in de lijst van meest grappige video's van YouTube Italië en komt na verloop van tijd zelfs bovenaan die lijst te staan. Ook bereikt de video de negenentwintigste plek op de lijst van meest bekeken video's op YouTube Italië. Op 6 november vraagt een kijker, Silvia Barabino, om de verwijdering van de video. Dit verzoek wordt op 7 november herhaald door de Post en Communicatie Politie, gevestigd te Rome. Diezelfde dag wordt de video verwijderd door YouTube. Er wordt door een aantal gebruikers beweerd dat zij al eerder melding hebben gemaakt van deze video, echter dit is niet onomstotelijk vast komen te staan tijdens het proces.

Geen van de Google medewerkers is op enigerlei wijze direct betrokken bij het vervaardigen of plaatsen van de video, noch hadden zij kennis van de plaatsing of van de inhoud van de video. Wel is Google, inc eigenaar van YouTube en is Google Italië een vestiging van Google Inc. Bovendien is Google Italië verantwoordelijk voor YouTube Italië en zijn de gedaagden verantwoordelijk voor een deel van het beleid van YouTube Italië.

¹ De uitspraak is te vinden op <http://bit.ly/c8DwSF>. Aangezien de uitspraak meer dan 100 pagina's bevat is de tekst hier in samengevatte vorm weergegeven. Let-

terlijke citaten zijn tussen aanhalingstekens geplaatst. De samenvatting en de vertaling van de letterlijke citaten zijn uitgevoerd door Bart van der Sloot.

YouTube's uploadproces kenmerkt zich door het ontbreken van enige voorafgaande controle. Een ieder kan een account aanmaken en vervolgens video's plaatsen. Dit proces verschaft de gebruikers van YouTube derhalve een zeer grote vrijheid. Deze vrijheid draagt er aan bij dat YouTube is uitgegroeid tot één van de meest succesvolle internetplatforms van dit moment. Dit succes, het aantal gebruikers en het aantal video's dat op YouTube te vinden is, heeft een gunstig effect op de winst die zij maakt. *A contrario* zou YouTube niet zo populair en winstgevend zijn als nu het geval is, indien de video's voor plaatsing op YouTube zouden worden gecontroleerd op hun inhoud.

Ondanks het ontbreken van preventieve controle heeft YouTube wel een aantal voorzorgsmaatregelen getroffen. De gebruikersvoorwaarden van YouTube stellen dat het materiaal dat wordt geupload op YouTube niet illegaal mag zijn en derhalve geen auteurs- of privacyrechten mag schenden en geen laster of smaad mag bevatten. Daarnaast kent YouTube het zogenoemde 'flag'-systeem, waarbij een gebruiker van YouTube een waarschuwing kan sturen ten aanzien van een video waarvan hij betwijfelt of deze aan de gebruikersvoorwaarden van YouTube voldoet. Deze video wordt binnen 24 uur bekeken door een YouTube-medewerker en bij schending van de gebruikersvoorwaarden verwijderd. Deze procedure is ook in het onderhavige geval gevolgd.

3. Wettelijk kader

Wetboek van strafrecht (Codice Penale):

Artikel 40 (Causaliteit)

Niemand wordt gestraft voor een feit dat door de wet wordt gekwalificeerd als misdrijf, in het geval de schadelijke of gevaarlijke handeling, noodzakelijk voor de kwalificatie 'misdrijf', niet het gevolg is van zijn handelen of nalaten. Het niet naleven van wettelijke verplichtingen om schade te voorkomen staat gelijk aan het veroorzaken van de schade.

Artikel 595 (Laster)

Iedereen, buiten de gevallen genoemd in het vorige artikel, die communiceert met meerdere personen en daarmee de reputatie van een ander schaadt, wordt gestraft met een gevangenisstraf van hoogstens een jaar of een boete van maximaal € 1032,-. Indien de inbreuk eruit bestaat iemand te betichten van een bepaald feit, is de straf een gevangenisstraf van ten hoogste twee jaar of een boete van ten hoogste € 2065,-. Als de overtreding is begaan door middel van de drukpers of een andere publicatievorm, of door een openbare handeling, is de straf een gevangenisstraf van zes maanden tot drie jaar of een boete van niet minder dan € 516,-. Als de laster een politiek, administratief of juridisch orgaan betreft of één van haar vertegenwoordigers of een college belast met autoriteit, wordt de straf verhoogd.

Wet op de Privacy (Code della privacy – Hierin is onder andere Richtlijn 95/46/EG betreffende de bescherming van data geïmplementeerd):

Artikel 4 (Definities)

Paragraaf (1)

(a) 'verwerking' betekent elke operatie of operaties, met of zonder elektronische middelen, betreffende het verzamelen, registreren, organiseren, opslaan, raadplegen, ontwikkelen, selecteren, uitnemen, vergelijken, gebruiken, koppelen, blokkeren, communiceren, verspreiden, verwijderen en vernietigen van data, zowel in een database als daarbuiten.

(b) 'persoonlijke informatie' betekent iedere informatie waarmee natuurlijke personen, juridische personen, entiteiten of bedrijven, worden geïdentificeerd of zijn te identificeren, direct of indirect, door verwijzing naar deze informatie, ook indien het, het persoonlijk identificatie nummer betreft.

[...]

(d) 'gevoelige informatie' betekent persoonlijke informatie die het ras of de etniciteit, religie, filosofie of ander geloof, politieke mening, lidmaatschap van partijen, vakbonden en religieuze, filosofische of politieke organisaties of de gezondheid en het seksuele leven van een persoon kan onthullen.

[...]

(f) 'datacontroller' is een natuurlijk persoon, een rechtspersoon, een publiek orgaan, instelling of organisatie of een andere entiteit met bevoegdheden, ook in samenwerking met anderen, die beslist over het doel, over de methoden van verwerking van de persoonlijke data en over de instrumenten die daarbij gebruikt worden, met inbegrip van de bescherming van de veiligheid.

(g) 'dataprocessor' is een natuurlijk persoon, een rechtspersoon, een publiek orgaan, instelling of organisatie of een andere entiteit die persoonlijke data verwerkt op verzoek van de datacontroller.

Artikel 5 (Onderwerp en toepassingsgebied)

1. Deze wet regelt de verwerking van persoonsgegevens, waaronder gegevens in het buitenland gehouden, uitgevoerd door een ieder die is gevestigd in Italië of op een plaats onder de soevereiniteit van Italië.

2. Deze wet is ook van toepassing op de verwerking van persoonsgegevens door iedereen gevestigd op het grondgebied van een land buiten de Europese Unie, waarbij gebruik wordt gemaakt van apparatuur, elektronisch of anderszins, die op het grondgebied van Italië staat, met uitzondering van het geval dat de apparatuur alleen gebruikt wordt voor de doorvoer van informatie binnen de Europese Unie. In het geval deze wet van toepassing is, zal de verantwoordelijke voor de gegevensverwerking een representant aanwijzen, gevestigd op het grondgebied van de staat, om de bepalingen inzake de verwerking van persoonsgegevens te implementeren.

3. De verwerking van persoonsgegevens door natuurlijke personen uitsluitend voor persoonlijke doeleinden, is alleen onderworpen aan deze wet als de gegevens zijn bestemd voor de systematische communicatie of verspreiding. De bepalingen omtrent aansprakelijkheid en veiligheid van de gegevens, zoals vermeld in artikelen 15 en 31, zijn in ieder geval van toepassing.

Artikel 31 (Beveiligingsverplichtingen)

1. Met inachtneming van de kennis met betrekking tot de technische mogelijkheden, de soorten gegevens en de specifieke kenmerken van de verwerking, moeten persoonsgegevens zo worden verwerkt, opgeslagen en gecontroleerd dat doormiddel van passende en preventieve veiligheidsmaatregelen, het risico van vernietiging of verlies van de data, al dan niet per ongeluk, van onbevoegde toegang tot data of van dataverwerking die niet is toegestaan of niet in overeenstemming is met de doeleinden van het verzamelen van die data, tot een minimum wordt beperkt.

Artikel 167 (Onrechtmatige gegevensverwerking)

1. Uitgezonderd het geval van een ernstige misdaad, kan een ieder die met oog op persoonlijk gewin of profijt ten behoeve van anderen of met het doel om andere schade te berokkenen persoonsgegevens verwerkt in strijd met artikelen 18, 19, 23, 123, 126 en 130, of krachtens artikel 129, worden bestraft, in het geval er schade is geleden, met een gevangenisstraf van zes tot achttien maanden, of, als het om communicatie of verspreiding gaat, met een gevangenisstraf van zes tot vierentwintig maanden.

2. Uitgezonderd het geval van een ernstige misdaad, kan een ieder die met oog op persoonlijk gewin of profijt ten behoeve van anderen of met het doel om anderen schade te berokkenen, persoonsgegevens verwerkt in strijd met artikelen 17, 20, 21, 22 paragrafen 8 en 11, 25, 26, 27 en 45, worden bestraft, indien er schade is geleden, met een gevangenisstraf één tot drie jaar.

Decreet van 9 april 2003, nummer 70 (Decreto legislativo 9 aprile 2003, n. 70 -Implementatie van de E-Commerce Richtlijn):

Artikel 16 (Verantwoordelijkheid voor de opslag van informatie - hosting)

1. Wanneer een dienst van de informatiemaatschappij bestaat uit de opslag van de door een afnemer van de dienst verstrekte informatie is de dienstverlener niet aansprakelijk voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat de dienstverlener:

- geen daadwerkelijke kennis had van de onwettige activiteit of informatie en, met betrekking tot een vordering tot schadevergoeding, geen kennis heeft van feiten of omstandigheden waaruit het onwettige karakter van de activiteiten of informatie duidelijk blijkt;
- zich niet bewust is van de onwettige activiteit, en zodra hij van het bovenbedoelde daadwerkelijk kennis heeft of beseft

krijgt, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken.

2. Lid 1 is niet van toepassing in het geval de afnemer van de dienst op gezag of onder toezicht van de dienstverlener handelt.

3. De rechterlijke en administratieve autoriteiten kunnen in een spoedeisend geval verlangen dat de dienstverlener het verrichten van werkzaamheden als in paragraaf 1 bedoeld, te beëindigen of te voorkomen dat de schendingen voortduren.

Artikel 17 (Geen algemene toezichtsverplichting)

1. Met betrekking tot de levering van de in de artikelen 14, 15 en 16 bedoelde diensten, hebben de dienstverleners 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.

2. Onverminderd de bepalingen van de artikelen 14, 15 en 16, is de aanbieder verplicht:

- onverwijld de rechterlijke of administratieve autoriteiten met toezichthoudende taken te informeren, indien de aanbieder kennis heeft van vermeende onwettige activiteiten of materiaal afkomstig van afnemers van zijn dienst;
- onverwijld informatie te verstrekken op verzoek van de bevoegde autoriteiten waarmee de afnemers van hun dienst met wie zij een opslagovereenkomst hebben gesloten, kunnen worden geïdentificeerd.

3. De dienstverlener is aansprakelijk voor de inhoud van dergelijke diensten wanneer, hij nalaat op verzoek van een rechtelijke of administratieve instantie die bevoegd is toezicht te houden, materiaal te verwijderen of toegang daartoe te voorkomen, of wanneer de dienstverlener die kennis had van het onwettige of schadelijke karakter voor derden van het materiaal of de activiteit, heeft nagelaten de bevoegde autoriteiten te informeren.

4. Rechterlijk oordeel

(1) Territorialiteit

Als preliminair verweer voert de verdediging aan dat Google Italië niet onder de jurisdictie van de Milanese rechter valt aangezien Google Inc., gevestigd op Amerikaans grondgebied, verantwoordelijk was voor de gegevensverwerking en ook de feitelijke gegevensverwerking plaats heeft gevonden op Amerikaans grondgebied. De rechter gaat hier echter niet op in en stelt dat als er sprake is van onrechtmatige gegevensverwerking, in de zin van artikel 167 Wet op de Privacy, moet worden gekeken naar de vereisten van artikel 5 van diezelfde wet. Dat artikel verklaart de wet van toepassing op de verwerking van persoonsgegevens uitgevoerd door een ieder die is gevestigd in Italië. Aangezien het kantoor van Google Italië is gevestigd in Milaan acht het hof zich bevoegd om uitspraak te doen in deze zaak.

(2) Laster

Als preliminair verweer wordt door de verdediging aangevoegd dat voor laster, artikel 595 van het Wetboek voor Strafrecht, er een verzoek tot vervolging van de beledigde persoon moet liggen. Deze was in casu afwezig. De rechter wijst dit verweer echter af daar niet alleen de jongen, of zijn vader, maar iedereen met het syndroom van Down wordt aangevallen en beledigd door deze video.

De rechter oordeelt vervolgens op basis van de videobeelden dat de getoonde situatie geen spelsituatie is, maar een situatie betreft waarin een groep jongeren een gehandicapt kind belaagt en bedreigt. Volgens de rechter staat buiten kijf dat de inhoud van de video zeer beledigend is voor de gehandicapte jongen. Ook de tekst die is geplaatst onder de naam van de organisatie Vivi Down is lasterlijk.

Vaststaat dat als YouTube alle bestanden preventief had gecontroleerd en gefilterd, de schade niet zou zijn ontstaan of van minder grote aard zou zijn geweest dan nu het geval is. Bij de vraag of YouTube voldoet aan zijn zorgplicht door de implementatie van een reactief beleid moet in ogenschouw worden genomen dat YouTube als content provider of als actieve hosting provider moet worden gekwalificeerd en derhalve een grotere zorgplicht heeft dan een passieve hosting provider. De aanklager meent dat een actieve hosting provider ook de plicht heeft om preventief te filteren, terwijl de verdediging, met een verwijzing naar de E-Commerce richtlijn, meent dat een provider geen plicht heeft om preventief te filteren.

De rechter komt tot het oordeel dat het artikel omtrent laster is geschreven voor primaire aansprakelijkheid en niet voor secundaire aansprakelijkheid. Het artikel ziet op de directe schade die wordt toegebracht door personen, niet op het doen of nalaten van derdeprijzen om deze schade te voorkomen. De voorbereiding van de reikwijdte van dit artikel door het openbaar ministerie vindt de rechter dan ook onjuist in het kader van artikel 40 Wetboek van Strafrecht. Er rust derhalve volgens de rechter geen plicht op YouTube om materiaal preventief te controleren en te filteren. Slechts als de provider kennis heeft van het inbreukmakende karakter van het materiaal en hij de inbreuk kan verhelpen kan de provider aansprakelijk worden gesteld.

Wel stelt de rechter dat ook in de virtuele wereld vrijheid en rechtvaardigheid met elkaar in overeenstemming moeten worden gebracht. De rechter meent dat er zich nu een lacune in het recht bevindt. 'Daarom, in afwachting van een goede wet die een strafrechtelijke verantwoordelijkheid voor de digitale wereld creëert (wellicht met betrekking tot nalatige en toerekenbare controle), zit er niets anders op dan de verdachten vrij te spreken van het misdrijf onder het kopje A [laster], een misdaad die zoals ze thans is geformuleerd, in casu niet aanwezig is.'

(3) *Schending van de privacy*

De rechter stelt vast dat naar analogie met de eerdere privacywetgeving, onder 'verwerking' in artikel 167 Wet op de Privacy ook moet worden verstaan de meer algemene begrippen 'communicatie' en 'verspreiding'. Daarnaast blijkt uit jurisprudentie dat er vier elementen van belang zijn bij de beoordeling van het onrechtmatige karakter van de gegevensverwerking: (a) de verwerking van gevoelige informatie; (b) het ontbreken van toestemming van de persoon waarop de informatie betrekking heeft; (c) schade aan die persoon; (d) opzet van de persoon die de gegevens heeft verwerkt. Hierbij kan economisch gewin een vermoeden van schuld opleveren.

Over vereisten (a) en (c) is de rechter kort: daaraan is in casu geval voldaan. Ten aanzien van vereiste (a) merkt de rechter op dat de video weliswaar het Syndroom van Down aan de jongen toeschrijft, terwijl hij aan autisme lijdt, maar dat er desondanks sprake kan zijn van gevoelige informatie die wordt verwerkt, indien er informatie wordt verspreid over de algemene gezondheid van een persoon. Dit was in casu het geval.

Ten aanzien van vereiste (d) wijst de verdediging er op dat zij een gratis dienst levert en geen winst maakt direct gerelateerd aan het publiceren van informatie. De openbaar aanklager wijst er daarentegen op dat YouTube wel degelijk winst maakt met deze dienst door reclameinkomsten, bijvoorbeeld via het programma AdWords. Deze reclameinkomsten zouden substantieel minder zijn als YouTube de inhoud van de bestanden vooraf zou controleren en zou filteren. De rechter stelt vast dat Google door middel van AdWords, woordherkenning en systematisering, informatie kan beheren, indexeren, organiseren en commerciële links kan exploiteren. Bovendien verzamelt Google informatie ten behoeve van de doorverkoop aan adverteerders. Google had derhalve een duidelijk financieel oogmerk om de informatiestroom zo groot en zo breed mogelijk te houden. Deze indicatoren wijzen volgens de rechter op '[...] een duidelijke en bewuste acceptatie van het grote risico van de data-integratie en -verspreiding, juist ook van gevoelige data die extra bescherming behoeven; dit risico en de duidelijke kennis daarvan werd geaccepteerd niet alleen, maar ook uit oogmerk van economisch gewin. Simpel gezegd: het is niet het schrijven op de muur waarmee de eigenaar een misdaad begaat, maar wel de commerciële exploitatie daarvan, zij het in bepaalde gevallen en onder bepaalde omstandigheden.'

Ten aanzien van vereiste (b) is de vraag wie er verantwoordelijk is voor het ontbreken van de toestemming van de autistische jongen. Deze plicht valt op de datacontroller en niet op de dataprocessor. De verdediging werpt op dat YouTube slechts een neutrale intermediair is. De rechter meent echter dat YouTube niet uitsluitend als neutrale intermediair kan worden gekwalificeerd aangezien het ook data selecteert en organiseert. 'Het is dus duidelijk dat de *actieve hoster of de content provider*, zoals u wilt, een hoger niveau van plichten zal hebben dan het niveau van een simpele *host provider of service provider of access provider*: dat het onvermijdelijk is dat zij de beheerder worden van de data blijkt al uit het enkele feit dat de gegevens worden georganiseerd, geselecteerd en kenbaar wordt gemaakt, en daarmee niet meer een vloed van niet van elkaar te onderscheiden data vormt, waarvan men de inhoud niet kent en waarvan men de inhoud ook niet hoeft te kennen [...]' YouTube valt derhalve wel degelijk onder het regime van de Wet op de Privacy.

De rechter oordeelt echter dat YouTube geen plicht heeft om het materiaal preventief te controleren en te filteren, wel heeft het de plicht om adequate voorzorgsmaatregelen te nemen om te zorgen dat haar gebruikers de wet niet overtreden. Ten aanzien daarvan is YouTube in gebreke gebleven. Weliswaar heeft zij haar gebruikers er op gewezen dat voor de publicatie van de persoonsgegevens van anderen toestemming is vereist, toch kan YouTube volgens de rechter de verantwoordelijkheid voor de privacyschending niet afschuiven op haar gebruikers met een verwijzing naar de algemene voorwaarden, aangezien de inhoud daarvan volgens de rechter onvoldoende helder van aard is en daarin onvoldoende duidelijk wordt welke plichten de gebruiker heeft na ondertekening. 'Het is daarom duidelijk, naar de mening van de schrijver, dat het niet voldoende is om aan de plichten die de wet oplegt te voldoen, door informatie omtrent de plichten die in de Wet op de Privacy zijn opgetekend te verbergen in de algemene voorwaarden die vaak onbegrijpelijk zijn, zowel wat betreft de inhoud als de wijze waarop de gebruiker is onderworpen aan deze algemene voorwaarden bij de 'aanvaarding' daarvan; dergelijk gedrag, met als doel om contractuele verplichtingen te minimaliseren en de onwil om te communiceren, constitueren een soort van 'vooropgezet alibi' aan de kant van de persoon/website en sluit derhalve geen negatieve beoordeling van het gedrag van de gebruikers uit.' YouTube heeft daarom niet voldaan aan de zorgplichten die een actieve hosting provider in acht moet nemen.

(4) *Oordeel*

De rechter spreekt alle gedaagden vrij van laster en veroordeelt Drummond, De los Reyes en Fleischer tot zes maanden voorwaardelijk voor schending van de Wet op de Privacy.

Noot

Bart van der Sloot

Mr. drs. B. van der Sloot is onderzoeker aan het Instituut voor Informatierecht van de Universiteit van Amsterdam.

Deze uitspraak van de Italiaanse rechter is in meerdere opzichten van belang. De uitspraak laat zien dat de Europese regelgeving, die in Italië zonder veel af te wijken is geïmplementeerd, in sommige opzichten moeilijk toe te passen is op nieuwe situaties en nieuwe technologische toepassingen. Deze constatering zal hier worden besproken aan de hand van de Privacyrichtlijn (Richtlijn 95/46/EG) en de E-Commercerichtlijn (Richtlijn 2000/31/EG).

De Privacyrichtlijn heeft onder andere ten doel datasubjecten te beschermen tegen gegevensverwerking door anderen. Hiertoe maakt de richtlijn een onderscheid tussen de gegevensverwerker (dataprocessor) en de verantwoordelijke voor de gegevensverwerking (datacontroller). Artikel 2d van die richtlijn bepaalt dat de verantwoordelijke de (rechts)persoon is die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Artikel 2e bepaalt dat de gegevensverwerker de (rechts)persoon is die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt. Dit verschil is relevant omdat de verantwoordelijke een aantal verplichtingen krijgt opgelegd met betrekking tot het verwerken van persoonsgegevens. Een van de belangrijkste hiervan, die ook in casu speelt, is de verplichting om toestemming te vragen voor publicatie van degene waarover in de data (gevoelige) persoonsgegevens worden verstrekt. De vraag die in deze zaak speelt, is wie de verplichting had om de toestemming van het autistische kind te vragen: de scholieren die het filmpje hebben geplaatst, YouTube of beide. Om te bepalen wie de verantwoordelijke is, is relevant wie het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Anders dan vroeger is dit onderscheid thans niet altijd helder te trekken. Enerzijds kan worden gesteld dat het YouTube is die de middelen voor de gegevensverwerking bepaalt en deze aanbiedt als een service op het internet. Anderzijds kan worden gesteld dat de gebruiker van YouTube dit platform heeft uitgekozen om zijn gegevens te verwerken. Hij had hier ook van af kunnen zien of een ander platform kunnen kiezen om zijn gegevens te laten verwerken. Enerzijds heeft YouTube een doel met betrekking tot de gegevensverwerking, namelijk een (afgeleid) financieel oogmerk. Anderzijds heeft de gebruiker van YouTube een doel met betrekking tot de gegevensverwerking, namelijk het openbaar maken van gedachten, informatie of meningen. Hieruit blijkt dat het onderscheid tussen de dataverwerker en de verantwoordelijke, anders dan voorheen, lang niet altijd helder te trekken is. Dit komt zowel doordat het materiaal steeds meer dan voorheen door 'amateur datacontrollers' op het internet

wordt geplaatst, die bijvoorbeeld hun privé-filmpjes of -foto's op hun eigen YouTube- of Facebookpagina plaatsen,¹ als doordat degenen die voorheen werden gezien als de verantwoordelijke, de site-houders, zich steeds actiever zijn gaan opstellen en hun positie er steeds minder één is van een neutrale intermediair. Bij het eerste punt zal hieronder worden stilgestaan, bij het tweede punt zal worden stilgestaan in het gedeelte over de E-Commercerichtlijn.

Aangezien het onderscheid tussen de verantwoordelijke en de verwerker steeds moeilijker te trekken is, rijst de vraag wie er moet worden belast met de verplichtingen die er rusten op de verantwoordelijke. Ten aanzien van YouTube kan worden gesteld dat, zoals de Italiaanse rechter ook heeft vastgesteld, het bedrijf een oogmerk heeft om winst te genereren. Deze winst is echter niet direct gekoppeld aan het materiaal dat op YouTube zelf verschijnt, maar aan de persoonsgegevens die zij verkrijgt van de bezoekers van YouTube. Deze informatie kan worden gebruikt voor *behavioural advertising*, oftewel persoonsgerichte reclame. YouTube heeft derhalve niet zozeer een doel om de filmpjes op haar site te verwerken, als wel om de gegevens te verwerken van haar klanten. Dat eerste is slechts een secundair belang. Dit sluit aan bij de opinie van de Artikel 29 Werkgroep dat hosting providers gegevensverwerkers zijn ten aanzien van de gegevens die hun klanten plaatsen op hun site, maar als verantwoordelijke vallen aan te merken ten aanzien van de persoonsgegevens van hun klanten die zij opslaan en verwerken.² Deze opinie wordt bevestigd door de Italiaanse rechter. YouTube heeft volgens hem geen plicht om vooraf toestemming te vragen van alle op de video's getoonde personen, een plicht die wel op de verantwoordelijke rust. De rechter merkt ten overvloede op dat dit voor YouTube ondoenlijk zou zijn.

Het is echter tevens de vraag of de gebruikers van YouTube in aanmerking komen voor de positie van verantwoordelijke. Als dit het geval zou zijn, zouden zij de toestemming van de op de video vertoonde personen moeten vragen alvorens tot publicatie over te gaan. Weliswaar is dat in casu niet bezwaarlijk, maar men bedenke dat op YouTube vele video's staan waar wildvreemde voorbijgangers worden gefilmd, bijvoorbeeld in het kader van onschuldige vakantievideo's. Het is ondoenlijk voor bijvoorbeeld een Japanse toerist die een film van zijn bezoek aan de binnenstad in Amsterdam op YouTube zet, om willekeurige voorbijgangers om toestemming te vragen. Al snel zal immers van enkele van hen gevoelige persoonsgegevens worden getoond, waardoor niet artikel 7, maar het strengere regime van artikel 8 van de Privacyrichtlijn van toepassing is. Daardoor geldt er geen uitzondering op het toestemmingsvereiste voor het geval dat de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde aan wie de gegevens worden verstrekt. Het anonimiseren is wellicht even bezwaarlijk door het arbeidsproces en de verandering in toon en sfeer van de video. Bovendien vallen er op de verantwoordelijke een aantal verplichtingen die men intuïtief niet typisch bij de YouTube-gebruiker zou leggen. Artikel 6 van de Privacyrichtlijn bepaalt bijvoorbeeld dat de verantwoordelijke verplicht is er zorg voor te dragen dat de verwerkte gegevens nauwkeurig zijn en zo nodig worden bijgewerkt en dat alle redelijke maatregelen worden getroffen om de gegevens die onnauwkeurig of onvolledig zijn uit te wissen of te corrigeren. Artikel 17 bepaalt dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer dient te leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking. Tot slot het voorbeeld van artikel 18, dat bepaalt dat de verantwoordelijke de toezichthoudende autoriteiten moet inlichten voordat wordt overgegaan tot volledig of gedeeltelijk geautomatiseerde verwerkingen van gegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden zijn bestemd. Dit zijn slechts enkele aanwijzingen dat de amateurgebruiker van het internet niet de eerst-aangewezen persoon

is om als verantwoordelijke te worden gekwalificeerd. Er zijn uiteraard meer professionele partijen actief op het internet waarbij deze kwalificatie wel gerechtvaardigd zou zijn, maar uit het voorgaande blijkt dat de positie van verantwoordelijke in het geval van YouTube doorgaans aan niemand toekomt. Wil men de juridische *idée fixe*, dat voor iedere handeling een verantwoordelijke en voor elke geleden schade een aansprakelijke is, handhaven dan behoeft de richtlijn enige aanpassing.³

Tot slot is ook de locatiegebondenheid van de Privacyrichtlijn niet in alle gevallen meer goed toepasbaar op de bestaande praktijk. Artikel 4 bepaalt het nationale recht van toepassing indien de verwerking van persoonsgegevens wordt verricht in het kader van de activiteiten van een vestiging op het grondgebied van de Lidstaat van de voor de verwerking verantwoordelijke of indien de voor de verwerking verantwoordelijke persoon niet gevestigd is op het grondgebied van de Gemeenschap en voor de verwerking van persoonsgegevens gebruik maakt van al dan niet geautomatiseerde middelen die zich op het grondgebied van genoemde Lidstaat bevinden, behalve indien deze middelen op het grondgebied van de Europese Gemeenschap slechts voor doorvoer worden gebruikt. De verwerking van gegevens is tegenwoordig echter vaak niet meer aan één specifieke locatie gebonden. Door het gebruik van technieken als *'cloud computing'* en het gebruik van *'grids'* is niet altijd evident op welke locatie de daadwerkelijke gegevensverwerking heeft plaatsgevonden. Ook in casu speelt de locatie van de gegevensverwerking een rol. De veroordeelde werknemers van Google Italië wijzen er op dat de gegevensverwerking in de Verenigde Staten plaatsvond en dat niet zij, maar Google Inc. verantwoordelijk was voor deze verwerking. Het eerste wordt niet betwist, wel merkt de rechter op dat deze gegevensverwerking plaatsvond ten behoeve van Google Italië. Hij verklaart deze dependance als een zelfstandig bedrijf, in het kader van wiens activiteiten de verwerking van gegevens plaatsvond. De openbaar aanklager doet het verweer van Google Italië dat zij geen invloed heeft op de gegevensverwerking af als de truc van de Chinese dozen (*scatole Cinesi*). Dit is een Italiaans gezegde dat verwijst naar dozen die, net als baboeska poppetjes, in elkaar kunnen worden geschoven. Alle aparte poppetjes, in dit geval een metafoor voor de verschillende dependances van Google, kunnen op het moment dat dit wenselijk is in het grotere poppetje worden geschoven. Dit terwijl de aanklager meent dat de verschillende dependances wel degelijke afzonderlijke entiteiten zijn die medeverantwoordelijk zijn voor de gegevensverwerking op Amerikaans grondgebied. Dit sluit aan bij zowel de Europese rechtspraak als de opinie van de Artikel 29 Werkgroep.⁴ Toch lijkt het onaannemelijk dat de veroordeelde bestuurders van Google Italië enige vorm van invloed of zeggenschap hadden over het proces en de manier waarop de gegevens werken verwerkt, omdat dit wel degelijk wordt aangestuurd door Google Inc. Zowel met betrekking tot de locatie van de daadwerkelijke gegevensverwerking als met betrekking tot de locatie van de daarvoor verantwoordelijke kan dus twijfel en discussie bestaan in relatie tot de formulering van de Privacyrichtlijn en de huidige rechtspraak.

Daarnaast roept deze zaak ook ten aanzien van de gebezigde terminologie in de E-Commercerichtlijn een aantal vragen op. De richtlijn biedt internetproviders een zogenoemde *safe harbour*, die hen uitsluiting van aansprakelijkheid biedt voor onwettige handelingen van hun gebruikers over hun netwerk. De richtlijn maakt een onderscheid tussen *'mere conduit'*-providers, die slechts verantwoordelijk zijn voor de toegang tot het internet of slechts zorgen voor de transmissie van materiaal over hun netwerk, providers die zich bezighouden met caching, de tijdelijke opslag van materiaal op de computer van de gebruiker, en hosting providers, die mogelijkheden tot opslag van materiaal op het netwerk bieden. Om aansprakelijkheid te ontlopen moeten de laatste twee providers meewerken aan de zogenoemde Notice-and-Take-Downprocedure, waarin de provider op het onwettige karakter van bepaald materiaal kan worden gewezen door een belanghebbende en hij het materiaal vervolgens onmiddellijk van

1 Artikel 29 Werkgroep, *Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'* (WP169), Brussel: 16 februari 2010. Artikel 29 Werkgroep, *Advies 5/2009 over online sociale netwerken* (WP163), Brussel: 12 juni 2009. CBP, *Richtnoeren: publicatie van persoonsgegevens op internet*, Den Haag: december 2007.

2 Artikel 29 Werkgroep, *Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'* (WP169), Brussel: 16 februari 2010, p. 29.

3 Zie daaromtrent ook: HvJ 6 november 2003 (Case C-101/01), *Lindqvist*.

4 Artikel 29 Werkgroep, *Advies 3/2009 over de ontwerpbeschikking van de Commissie inzake modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG (van de voor de gegevensverwerking verantwoordelijke naar de verwerker)* (WP161), Brussel: 5 maart 2009.

5 B. van der Sloot: 'De verantwoordelijkheid voorbij: de ISP als verlengstuk van de overheid.' *Mediaforum* 2010-5, p. 157-161.

zijn netwerk moet verwijderen. Deze actieve handeling wordt ook wel de positieve verplichting van de internet tussenpersoon genoemd.⁵ Ook mag de provider zich niet bewust zijn van feiten of omstandigheden die op het onrechtmatige karakter van bepaald materiaal kunnen wijzen. Dit wordt in de Digital Millennium Copyright Act sectie 512, dat een soortgelijke *safe harbour* implementeert, de *'red flag'*-test genoemd. De mere conduit-provider heeft geen positieve verplichting om aanspraak te maken op de *safe harbour*. Wel geldt voor alle providers dat zij aan de negatieve verplichtingen van de *safe harbour* moeten voldoen. Dit betekent dat zij niet actief betrokken mogen zijn bij de onwettige activiteit, bijvoorbeeld door de transmissie van het materiaal te initiëren, de inhoud van het materiaal te wijzigen of de ontvangers van het materiaal te selecteren.

Over de categorisering bestaat al langer discussie. Zo ontbreekt in de Europese Richtlijn een categorie voor *'selection intermediaries'*, waaronder bijvoorbeeld zoekmachines vallen, die wel in de Digital Millennium Copyright Act is opgenomen.⁶ Daarnaast staat de categorie van de mere conduit-providers ook onder druk. In Europa valt hieronder de provider van een dienst die bestaat uit het doorgeven van door een afnemer van de dienst verstrekte informatie of uit het verschaffen van toegang tot een communicatienetwerk en in de Verenigde Staten valt hieronder de provider zich bezighoudt met *'transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections'*. Deze providers hebben slechts negatieve verplichtingen om in aanmerking te komen voor de *safe harbour*. Het verschaffen van toegang en het faciliteren van de transmissie van materiaal was ooit een duidelijk afgezonderde service die door een bepaald type provider werd verzorgd. Zij hielden zich niet bezig met het hosten of cachen van materiaal. Hede ten dage zijn er echter zeer weinig providers die zich uitsluitend met mere conduit bezighouden. Steeds vaker bieden zij hun klanten ook zogenoemde *'over the top'* services aan, zoals het filteren van spam, het hosten van persoonlijke pagina's of het aanbieden van e-mailservices. Dit roept de vraag op of de E-Commerce Richtlijn een onderscheid maakt tussen providers of tussen aangeboden diensten. Zou het eerste het geval zijn dan zou vrijwel geen enkele internet intermediair meer onder de mere conduit *safe harbour* vallen; zou het tweede het geval zijn, wat inderdaad de rechtspraktijk lijkt te zijn, dan zouden deze providers met betrekking tot hun mere conduit-diensten slechts negatieve verplichtingen hebben om onder de *safe harbour* te vallen, terwijl zij ten aanzien van hun *'over the top'*-diensten ook actieve verplichtingen zouden hebben.

Een derde discussiepunt met betrekking tot de terminologie van de richtlijn, die ook in casu aan de orde kwam, speelt ten aanzien van de categorie van de hosting provider. Oorspronkelijk, toen deze wetgeving zowel in Europa als in de Verenigde Staten werd vervaardigd, was ook deze categorie van providers vrij duidelijk omschreven. Er werd door providers opslagruimte aangeboden tegen betaling. De organisatie van het materiaal en de inhoud van de site werd aan de klant overgelaten. Tegenwoordig zijn er echter steeds meer sites, zoals Facebook en YouTube, die actief betrokken zijn bij de organisatie van het materiaal en de inrichting van de site. Steeds vaker wordt er daarom een onderscheid gemaakt tussen passieve hosting providers en actieve hosting provider, alhoewel de vraag blijft of dergelijke platformen überhaupt onder de definitie van hosting provider vallen. Ook in casu werd dit onderscheid gemaakt. Dit onderscheid heeft betrekking op de negatieve vereisten van artikel 14 E-Commerce Richtlijn. Steeds vaker wordt de actieve hosting provider een beroep op de *safe harbour* ontzegd omdat hij niet aan zijn negatieve verplichtingen zou voldoen. Zo besloot een Italiaanse rechter dat ten aanzien van de schending van intellectueel eigendom, Pirate Bay aansprakelijk kon wor-

den gesteld daar deze *'bittorrent tracker'* een actieve bijdrage leverde aan de inbreukmakende activiteiten door het bijhouden van lijsten van bittorrents en het indexeren van materiaal.⁷ In Frankrijk bepaalde een rechter uit Parijs ten aanzien van MySpace dat zij niet kon worden gezien als een passieve hosting provider, met als belangrijkste argument dat MySpace aan haar diensten geld verdiende.⁸ In de hier besproken zaak speelde zowel het geldelijke gewin, door middel van AdWords, als ook het feit dat YouTube data organiseert en systematiseert een belangrijke rol. In een onlangs verschenen arrest van het Hof van Justitie, stond ter discussie of Google aansprakelijk kon worden gesteld voor onrechtmatige advertenties die via Google AdWords werden geplaatst.⁹ Adverteerders kunnen via dat programma Google betalen om hun advertentie te tonen bij bepaalde zoekopdrachten in de zoekmachine. Zij mogen daartoe een aantal trefwoorden opgeven. In die zaak werd daarbij echter inbreuk gemaakt op de intellectuele eigendomsrechten van anderen. De vraag rees of Google nog wel als neutrale intermediair kon worden gekwalificeerd, aangezien zij informatie organiseert en systematiseert. Het Hof oordeelde dat: *'Om na te gaan of de aansprakelijkheid van de verlener van de zoekmachine-advertentiedienst krachtens artikel 14 van richtlijn 2000/31 kan worden beperkt, moet derhalve worden onderzocht of de rol van deze dienstverlener in die zin neutraal is dat zijn handelingen louter technisch, automatisch en passief zijn, wat impliceert dat hij geen kennis heeft van of controle heeft over de gegevens die hij opslaat. Wat de in de hoofdgedingen aan de orde zijnde zoekmachine-advertentiedienst betreft, blijkt uit het dossier en de beschrijving in de punten 23 en volgende van het onderhavige arrest dat Google, met behulp van door haar ontwikkelde software, de door adverteerders ingevoerde gegevens verwerkt en dat dit proces leidt tot de weergave van advertenties onder door Google gecontroleerde voorwaarden. Aldus bepaalt Google de volgorde van weergave op basis van met name de door de adverteerders betaalde vergoeding.'*¹⁰ In de Italiaanse zaak betrof het echter niet het illegale karakter van de advertenties zelf, maar van de op de website vertoonde video's. De Milanese rechter oordeelt analoog aan de uitspraak van het Hof van Justitie dat ook het materiaal op de website wordt geordend en gsystematiseerd. Dit valt onder andere af te leiden uit het feit dat YouTube zich bezighoudt met het maken van lijsten met de populairste en grappigste video's. Hieraan zouden ook de zoekalgoritmes van Google kunnen worden toegevoegd. Derhalve wordt YouTube door de Italiaanse rechter als actieve hosting provider gekwalificeerd. Zij heeft derhalve meer zorgplichten in acht te nemen dan in het geval zij als passieve hosting provider zou zijn gekwalificeerd. Eén van die zorgplichten is het afdoende en op transparante wijze informeren van haar gebruikers over hun wettelijke verplichtingen. Hieraan heeft YouTube in casu niet voldaan. Haar algemene voorwaarden, waarin deze verplichtingen zijn vervat, zijn niet afdoende leesbaar en transparant. Bovendien zijn de verplichtingen *'weggestopt'* in een verklaring die moeilijk te vinden is op de site en die wordt getekend door het aanvinken van een vakje. Dit oordeel sluit aan bij de steeds vaker en luider gehoorde kritiek dat de gebruikersvoorwaarden en privacyverklaringen van internetbedrijven te onduidelijk en onleesbaar zijn voor de normale internetgebruiker. Ook de ondertekening van een verklaring door het aanvinken van een vakje wordt, alhoewel rechtens juist door de aangehouden vormvrijheid van contracten, vaak als onwenselijk beschouwd.

De extra zorgplicht kan tot slot leiden tot de al vaker geconstateerde paradox dat providers die activiteiten ontplooiën om schadelijk materiaal actief op te sporen en te verwijderen, juist daarom aansprakelijk kunnen worden gesteld voor het illegale materiaal dat via hun netwerk wordt verspreid. Dit omdat zij enerzijds kennis hadden of moesten hebben van het onrechtmatige karakter van het materiaal of anderzijds omdat zij niet meer voldoen aan de negatieve verplichtingen die de E-Commerce Richtlijn als voorwaarde aan de *safe harbour* stelt. Dit kan bijvoorbeeld problematisch zijn voor providers die

6 J. van Hoboken: 'Legal space for innovative ordering: on the need to update selection intermediary liability in the EU.' *International journal of communications law and policy* 2009/13, p. 1-21.

7 Corte di Cassazione del 29 septembre 2009 (no. 49437/2009).

8 Tribunal de grande instance de Paris Ordonnance de référé 22 juin 2007.

9 HvJ EG 23 maart 2010 (zaken C-236/08 t/m C-238/08), *Google France*.

10 Overwegingen 114 en 115. Het Hof geeft hiermee geen definitief oordeel, maar verwijst de zaak terug naar de nationale rechterlijke macht. Ook zijn er andere overwegingen die de hier geciteerde overwegingen nuanceren. Overwegingen 116 tot en met 118 lezen: *'Opgemerkt dient te worden dat het enkele feit dat voor de zoekmachineadvertentiedienst moet worden betaald, dat Google de wijze van*

vergoeding bepaalt of dat zij algemene inlichtingen aan haar klanten verstrekt, niet ertoe kan leiden dat Google geen beroep kan doen op de in richtlijn 2000/31 vastgestelde vrijstellingen van de aansprakelijkheid. Ook het feit dat het geselecteerde trefwoord en het door een internetgebruiker ingevoerde zoekwoord overeenkomen, volstaat op zich niet om ervan uit te gaan dat Google kennis heeft van of controle heeft over de door adverteerders in haar systeem ingevoerde en op haar server opgeslagen gegevens. Wel relevant voor het in punt 114 van het onderhavige arrest bedoelde onderzoek daarentegen is de rol van Google bij het schrijven van de reclameboodschap die de advertentielink begeleidt, of bij de vaststelling of de selectie van trefwoorden.'

actief naar kinderpornografisch materiaal op hun netwerk zoeken. Weliswaar verklaart artikel 15 dat providers geen algemene verplichting tot filtering of tot opsporing van illegaal materiaal op hun netwerk mogen worden opgelegd (dit staat ook in relatie tot artikel 10 Europees Verdrag voor de Rechten van de Mens en de terughoudendheid met betrekking tot censuur), maar dit artikel is door een aantal landen niet geïmplementeerd in hun nationale wetgeving. Bovendien bestaat er een frictie tussen de negatieve verplichtingen en de zorgplichten van internetproviders.¹¹ Deze frictie wordt ook in deze zaak duidelijk. YouTube krijgt als actieve hosting provider extra zorgplichten opgelegd om haar klanten er op te wijzen dat zij zich aan de nationale wet- en regelgeving moeten houden. Dit kan onder andere door deze verplichtingen helder en duidelijk te formuleren in haar algemene voorwaarden en door deze verplichtingen op een plaats te tonen, bijvoorbeeld op de startpagina, waartoe de gebruiker gemakkelijk toegang heeft. Het probleem is echter dat YouTube juist door deze handeling te kennen geeft zich bewust te zijn van het feit dat er illegaal materiaal wordt verspreid op haar netwerk. Deze kennis is relevant ten aanzien van de 'red flag' test. Weliswaar heeft YouTube geen kennis van het illegale karakter van specifiek materiaal, maar dat is ook niet noodzakelijk. Er is hier eerder sprake van een glijdende schaal. Naarmate het de provider duidelijker wordt dat er een kans is dat er via zijn site illegaal materiaal wordt verspreid en naarmate de kans dat het materiaal een onwettig karakter heeft groeit, heeft hij meer en grotere zorgplichten om deze inbreuken te voorkomen.¹²

Indien er (veel) meer illegaal dan legaal materiaal wordt verspreid via een dienst dan moet de provider redelijkerwijs vermoeden dat het materiaal dat wordt geplaatst op zijn netwerk een illegaal karakter heeft en zal hij materiaal vooraf moeten filteren en controleren op zijn (on)wettige karakter. Dit is één van de redenen waarom sites als Napster niet of nauwelijks meer kunnen functioneren. Het argument dat door Napster werd aangevoerd, dat zij niet van ieder materiaal het wettige dan wel het onwettige karakter kende, werd door een rechter uit de Verenigde Staten van de hand gewezen omdat het businessmodel van Napster was gericht op en rekening hield met de grootschalige verspreiding van illegaal materiaal over zijn netwerk.¹³ Hiermee viel Napster onder de categorie van *contributory infringements*, een vorm van *secondary liability*, waarvoor de twee vereisten zijn: (1) kennis van de illegale handeling en (2) geldelijk gewin verbonden aan de illegale handeling. Alhoewel de Europese regelgeving deze vorm van secundaire aansprakelijkheid niet kent, is het precies deze redenering die de rechter in casu lijkt te volgen. Omdat YouTube video's niet vooraf controleert op hun (on)wettige karakter staan er zoveel video's op haar netwerk; omdat er zoveel video's op haar netwerk staan is YouTube zo populair geworden; omdat YouTube zo populair is geworden heeft YouTube zoveel klanten; omdat zij zoveel klanten heeft, heeft zij van zoveel mensen persoonsgegevens en omdat zij van zoveel mensen persoonsgegevens heeft kan zij zoveel winst maken via de doorverkoop van deze data.

11 B. van der Sloot: 'De verantwoordelijkheid voorbij: de ISP als verlengstuk van de overheid.' *Mediaforum* 2010-5, p. 157-161.

12 Vzf. Rb. Amsterdam 1 november 2007, LjN BB6926.

13 *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (Ninth Circuit, 2001).