Noot bij HvJ EU 15 september 2016, C-484/14 (Mc Fadden/Sony Music), gepubliceerd in IER 2017/13

Jacqueline Seignette

Het Langericht München stelt prejudiciële vragen over de reikwijdte van de mere conduit vrijstelling in artikel 12 van de e-commerce richtlijn (2000/31, geciteerd in ov. 9). Eiser Tobias McFadden heeft een onderneming in licht- en geluidsapparatuur. Het wifi netwerk van het bedrijf is bewust niet beveiligd om klanten van omringende winkels, voorbijgangers en buren op het bedrijf te attenderen. In 2010 doopt McFadden de url van zijn wifi netwerk om van 'mcfadden.de' naar 'freiheitstattangst.de' om de aandacht te vestigen op een demonstratie tegen privacyschending en buitensporige overheidscontroles. Zes weken later spreekt Sony Music McFadden aan wegens inbreuk op fonogrammenrecht omdat er muziek via een filesharing site is uitgewisseld met behulp van zijn wifi netwerk. McFadden zegt dat hij dat zelf niet was en vordert een verklaring van niet-inbreuk. Het Landgericht München overweegt McFadden indirect aansprakelijk te stellen als 'Störer' (*Störerhaftung*) omdat hij het netwerk niet beveiligd heeft, maar vraagt zich af of de mere conduit bepaling de mogelijkheid daartoe niet op één of andere manier inperkt.

Het Hof van Justitie beantwoordt eerst een aantal vragen over het toepassingsgebied van artikel 12. Het Hof grijpt voor de betekenis van 'dienst van de informatiemaatschappij' in artikel 12 terug naar richtlijn 98/34, dat bepaalt dat het moet gaan om diensten die gewoonlijk tegen vergoeding worden verricht. Het Hof heeft dit in eerdere uitspraken ruim uitgelegd en doet dat hier ook: als het netwerk gratis ter beschikking gesteld wordt om reclame te maken voor de eigen producten of diensten, dan is dat een 'dienst voor de informatiemaatschappij'. Voor toepassing van de vrijstelling is vervolgens niet nodig dat er een contractuele verhouding bestaat met de afnemer van de dienst en ook niet dat de dienstverlener reclamemiddelen gebruikt voor die dienst. Voldoende is dat de toegang het kader van het technisch, automatisch en passief proces van doorgifte niet te buiten gaat. Hieraan doet aldus het Hof niet af dat de Duitse taalversie spreekt over 'anbieten', dat zou kunnen refereren aan een aanbod tot contracteren en aan reclame. Voor de uitleg van een richtlijn moet naar alle taalversies worden gekeken en diverse andere taalversies gebruiken werkwoorden die niet refereren aan een aanbod tot contracteren of aan reclame (ov. 53).

Het Landgericht München wil ook weten of de mere conduit vrijstelling (artikel 12) net als de hosting vrijstelling (artikel 14) vereist dat de dienstverlener het inbreukmakende werk ontoegankelijk maakt zodra hij kennis heeft gekregen van het onrechtmatige karakter. Het Hof vindt van niet. Zowel de mere conduit als hosting vrijstelling vereisen dat de dienst een louter technisch, automatisch en passief heeft en dat de provider bij aanvang van de dienst geen kennis heeft van, of controle over, de informatie die wordt doorgegeven of opgeslagen. Artikel 12 vereist echter niet dat de access provider illegaal materiaal moet verwijderen als hij daar later alsnog kennis van verkrijg (ov. 64). Het Hof merkt daarbij op dat de access dienst vluchtig is, zodat de access provider dus "vaak" niet in staat zal zijn om de informatie nog te verwijderen als hij alsnog kennis krijgt van het onrechtmatige karakter (wel kennis, maar geen controle). Bij hosting ligt dat anders. Als de hosting provider bij aanvang van de dienst geen kennis heeft maar tijdens de opslag alsnog kennis krijgt, kan hij deze verwijderen en moet hij dat ook doen om voor de vrijstelling in aanmerking te komen (kennis en controle).

De aanname dat een access provider geen kennis en controle heeft, behoeft wel enige nuancering. Het is een gegeven dat de populairste muziek, films, tv series, ebooks en games illegaal op het internet te vinden zijn. Toegang tot internet betekent dus ook toegang tot deze werken. We vinden het echter onwenselijk als de access provider schadeplichtig zou worden als hij niet vooraf voor al die werken toestemming regelt. Iets anders is of de provider zonder meer mag weigeren om software te installeren die inbreukmakend materiaal kan identificeren en filteren.

SABAM probeerde jaren geleden om een internet provider en sociale media platform te verplichten om al het internet verkeer te filteren. Daar was volgens het Hof geen ruimte voor omdat dit de dienstverlener op hoge kosten zou jagen en het bovendien zou neerkomen op een algemene toezichtverplichting, wat volgens artikel 15 van de e-commerce richtlijn niet mag.[1] Inmiddels zijn we een aantal jaren verder en is filter technologie volwassen en wordt het op grote schaal commercieel toegepast. Gebruik van filtersoftware is voor bedrijven en consumenten een normale zaak geworden. Filters worden gebruikt om specifieke informatie uit te filteren, zoals spam, kindonvriendelijke informatie of kinderporno (content filters), om relevante informatie te vinden (zoekmachines, datamining) of om internet gebruikers gerichte informatie of reclame te kunnen toesturen die bij hun profiel past. Er wordt ook steeds meer software gebruikt om auteursrechtelijk beschermde content te identificeren, zoals het Content ID systeem van YouTube. Organisaties als Buma Stemra stellen ook herkenningssoftware ter beschikking waarmee omroepen, dj's en streaming diensten geautomatiseerd kunnen registreren welke muziek er wordt gebruikt.

Het past niet bij deze realiteit om tussenpersonen volledig te vrijwaren van de verplichting om filters toe te passen om inbreuk tegen te gaan. Bij opslagdiensten, zoals webhosting, marktplaatsen, social media platforms, cyberlockers en usenet diensten, groeit de rechtspraak in binnen- en buitenland toe naar een genuanceerde verplichting om maatregelen te nemen om inbreuken te voorkomen. Het Hof Amsterdam oordeelde in Brein/NSE dat usenet provider NSE naast een notice-and-take-down procedure aanvullende maatregelen moet nemen om inbreuken te weren. Een filter die usenet bestanden filtert op woorden in de headers kan zo een maatregel zijn en komt aldus het Hof niet in strijd met het algemene toezichtverbod van artikel 15 lid 1 van de e-commerce richtlijn.

De ontwerp DSM richtlijn die de Europese Commissie in september 2016 publiceerde, borduurt op deze ontwikkeling voort. Diensten van de informatiemaatschappij "die zich bezighouden met het opslaan van en het verlenen van publieke toegang tot grote hoeveelheden door hun gebruikers geüploade auteursrechtelijk beschermde werken of andere materialen" moeten passende en evenredige maatregelen treffen om door rechthebbenden aangewezen werken te weren, zoals technologieën voor herkenning van inhoud. Dit geldt ook als de dienst een beroep toekomst op de hosting vrijstelling van artikel 14.[2]

Geldt hetzelfde voor access providers? Mag een access provider weigeren om op verzoek van rechthebbenden een gratis app te installeren die voorkomt dat er via zijn wifi netwerk toegang wordt verleend tot websites waarvan de rechter heeft vastgesteld dat die substantieel worden gebruikt om illegaal materiaal uit te wisselen? Kan de rechter de access provider bevelen om de app toch te installeren plaatsen of om de betreffende websites te blokkeren? Het Hof van Justitie oordeelde in *UPC Telekabel Wien* dat een bevel tot blokkering van een inbreukmakende website op grond van artikel 8 lid 3 van richtlijn 2001/29 mogelijk is, mits de access provider zelf kan kiezen welke technische middelen hij daartoe aanwendt en hij aan het bevel kan ontkomen door aan te tonen dat hij hiertoe alle redelijke maatregelen heeft genomen. Voorwaarde is dat de maatregel het gebruik verhindert of minstens bemoeilijkt, dat het gebruikers ontmoedigt om inbreuk te maken en dat het rechtmatig gebruik niet nodeloos beperkt.[3]

Het Hof van Justitie overweegt in het onderhavige arrest dat uit artikel 12 lid 3 van de e-commerce richtlijn volgt dat de rechthebbende jegens de access provider kan vorderen dat de voortzetting van de inbreuk wordt verboden (ov. 79). De vraag is welke maatregel de provider dan moet nemen om aan dit bevel te voldoen. De verwijzende rechter gaat ervan uit dat de access provider maar drie mogelijkheden heeft: alle via een aansluiting door te geven informatie onderzoeken, de aansluiting

[1] HvJ EU 24 november 2011, C-70/10 (Sabam/Scarlet); HvJ EU 16 februari 2012, C-360/10 (Sabam/Netlog).
[2] Voorstel voor een richtlijn van het Europees Parlement en de Raad inzake auteursrechten in de digitale eengemaakte marktBrussel, 14.9.2016, COM(2016) 593 final, considerans 38 en artikel 13.
[3] HvJ 27 maart 2014, C-314/12, IER 2014/45, m.nt. S. Kulk.

blokkeren, of deze beveiligen met een wachtwoord. Het eerste zou aldus het Hof in strijd komen met het algemene toezichtsverbod van artikel 15 lid 1 van de e-commerce richtlijn (ov. 87). Het blokkeren van de internet aansluiting acht het Hof een te ernstige aantasting van de vrijheid van ondernemerschap omdat dit de facto zou betekenen dat de provider helemaal geen internet toegang meer kan bieden (ov. 88-89). Het Hof lijkt de maatregel zo te interpreteren dat de provider alle aansluitingen blokkeert, zodat er niemand meer toegang tot het wifi signaal heeft. De verwijzende rechter spreekt echter over een verbod om via een concrete internet aansluiting auteursrechtelijk beschermde werken te uploaden (prejudiciële vraag 9). Als de provider de aansluiting van een specifieke uploader moet blokkeren, kan hij zijn wifi netwerk nog steeds openstellen voor derden. Van een ernstige aantasting van de vrijheid van ondernemerschap lijkt mij in dat geval geen sprake.

Een wachtwoord vindt het Hof geen wezenlijke aantasting van de vrijheid van ondernemerschap en van de vrijheid van informatie van de gebruikers (ov. 91-92) . Het belemmert gebruikers niet om toegang te krijgen tot rechtmatige informatie en is voldoende doeltreffend, althans voorzover gebruikers hun identiteit moeten opgeven om een wachtwoord te krijgen. Deze voorwaarde kan hen er namelijk van weerhouden om inbreuk te maken, zo redeneert het Hof. De nationale rechter moet nagaan of dit echt zo is (ov. 96). Als dat zo is, creëert het toepassen van een wachtwoord een rechtvaardig evenwicht tussen de grondrechten, ervan uitgaande dat er geen andere maatregelen zijn om aan het bevel te voldoen (ov. 97, 100). Het Hof acht de registratie van gebruikers en de daaraan verbonden verplichtingen uit hoofde van de privacywetgeving in dat geval dus aanvaardbaar als middel ter bescherming van de intellectuele eigendom.

Kan een aanbieder van een wifi netwerk zich nu in alle gevallen disculperen door een wachtwoord te gebruiken? In cafés hoeft men zich meestal niet te registreren en ligt er een wachtwoord dat voor alle bezoekers hetzelfde is. Dat voldoet niet aan de eis die het Hof stelt. De gebruiker zal zich eerst moeten identificeren en een wachtwoord invoeren. Ook McFadden zal voorbijgangers aan zijn winkel eerst moeten laten registeren en een wachtwoord toekennen alvorens hen toegang tot het wifi netwerk te geven.

Een interessante vraag is hoe de grondrechtelijke afweging uitpakt als de rechthebbenden (bijvoorbeeld Brein) een gratis app ter beschikking stellen die zorgt voor automatische blokkering van één of meer filesharing sites via welke substantieel inbreukend materiaal wordt uitgewisseld. Het wifi netwerk kan dan gewoon worden aangeboden en uploaders kunnen toegang krijgen tot het wifi netwerk, maar zij kunnen alleen geen illegale bestanden meer uitwisselen via de betreffende site(s). De grondrechten van informatievrijheid en ondernemerschap lijken hiermee gewaarborgd. Het grondrecht van intellectuele eigendom wordt bovendien beter gewaarborgd dan met een wachtwoord, omdat het een doeltreffender middel is.

Later dit jaar zal het Hof in *Brein/Ziggo* antwoord geven op de vraag of een bevel tot blokkering ook kan worden gegeven met betrekking tot een bit torrent site als de ThePirateBay, die zelf geen inbreukmakend materiaal op haar server heeft staan, maar via torrent links wel toegang geeft tot substanteel inbreukmakend materiaal (in geval van ThePirateBay tenminste 90%). De A-G heeft intussen onder verwijzing naar *UPC Telekabel Wien* geconcludeerd dat dit in beginsel kan omdat ThePirateBay ondanks wetenschap van inbreukmakend materiaal doorgaat en daarom mede verantwoordelijk is voor de mededeling aan het publiek via de site. Maar ook als het Hof van Justitie die conclusie niet volgt, vindt de A-G dat de nationale rechter een bevel kan opleggen als dit evenredig is met de omvang en ernst van de inbreuken die door middel van de website worden gemaakt.[4]

[4] Conclusie A-G 8 februari 2017, C-610/15 (Brein/Ziggo).