

## **HC 5, 27-11-2018, Digitale overheid**

Bij het onderwerp digitale overheid zijn drie onderwerpen van belang:

- elektronische communicatie
- digitale besluitvorming
- digitale infrastructuur

De gemene deler van deze drie onderwerpen is het koppelen van bestanden/het doorsturen van gegevens.

### **Het koppelen van systemen**

Tegenwoordig is alles aan elkaar verbonden door vernetwerken en door het samenstellen en verrijken van informatie. Het doel is het voeren van een preventief en effectief beleid. Het verrijken van informatie en het voeren van een beleid daarop is proactief; het is snel en effectief.

Het koppelen van systemen zorgt ervoor dat de informatie klopt en het bewaart de integriteit en authenticatie van de informatie. Verder zorgt het voor transparantie dat de informatie niet voor verkeerde doeleinden wordt gebruikt (function creep).

In Nederland bestaat er een inlichtingenbureau. Dit bureau is opgericht bij wet. Ze maken daar op basis van SiRi (systeemrisicoanalyse) profielen van mensen.

### **Romet**

Romet had 1752 auto's op zijn naam staan. Hiervoor moest hij ook wegenbelasting betalen en een verzekering afsluiten voor elke auto. Dit heeft hij niet gedaan en als gevolg kreeg hij daar boetes voor. Hij kreeg geen uitkering, omdat de auto's gezien werden als bezit en de waarde van de auto's maakte hem zogenaamd rijk. De regering zei dat wat in de registratie staat waar is en het wijzigen van de gegevens met terugwerkende kracht in strijd is met de rechtszekerheid (van het systeem). Dit werd aangevoerd, omdat basisregistraties de grondslag voor vele besluiten vormen. Als er eenmaal begonnen wordt met wijzigen, zal het systeem compromitteren. Dit is dus een voorbeeld waarin het systeem boven de rechtszekerheid van een persoon gaat.

Romet ging naar het Europees Hof en zei dat zijn persoonlijke levenssfeer ernstig geschonden was. Het EHRM gaf hem gelijk, zij vond namelijk dat het niet snel genoeg in actie komen van de overheid zorgde voor ernstige schending van dit recht.

### **Kowsoleea**

Kowsoleea was een slachtoffer van identiteitsfraude. De oorzaak hiervan was onvoldoende vaststelling door de politie bij aanhouding van een ander (gevaarlijke geveerwapende man) die de naam van Kowsoleea opgaf als zijn eigen naam. De advocaat kreeg de gegevens niet gewijzigd. Uiteindelijk zijn de gegevens door een medewerker van het gerechtshof gewijzigd. Dit is een voorbeeld van de ketenproblematiek bij de overheid. Hele strikte wetstoepassing is dus niet altijd wenselijk, want dit kan leiden tot onbillijkheden. Digitalisering leidt tot deze strikte wetstoepassing, want een digitaal systeem maakt geen uitzonderingen en werkt altijd hetzelfde.

### **Publieke waarden**

Het grote vraagstuk is hoe je de publieke waarden in IT-systemen bouwt; dit is soms in wetgeving al een probleem. Het is van belang voor de private sector, maar bovenal voor de overheid, want die moet ervoor zorgen dat de systemen voldoen aan de criteria van de democratische rechtstaat: rechtszekerheid, gelijkheid, democratie en de dienende overheid.

### **IT-gebruik door de overheid**

Franken kwam in 1993 met de beginselen van behoorlijk IT-recht gebruik:

- beschikbaarheid → er moet sprake zijn van makkelijke toegang
- vertrouwelijkheid
- integriteit
- authenticiteit → de kwaliteit van het systeem en de gegevens
- flexibiliteit
- transparantie

Voor de burger moet het makkelijk zijn te gebruiken, transparant zijn, geen digitale dwangbuis zijn (digitaal formulier) en correctie en rechtsherstel moeten altijd mogelijk zijn. Het moet voor iedereen toegankelijk zijn. Als de overheid zich aan deze beginselen houdt, dan is er sprake van een behoorlijk bestuur.

### **Modernisering afd. 2.3 Awb**

Momenteel ligt er een voorstel bij de Raad van State om afdeling 2.3 van de Awb te moderniseren. Er zal dan geregeld worden dat de burger recht heeft op elektronische communicatie.

## **HC 6, 30-11-2018, Materieel strafrecht en IT**

### **Computercriminaliteit**

Binnenkort treedt de derde Wet Computercriminaliteit in. Deze wet geeft een overzicht van strafbepalingen ter bestrijding van computercriminaliteit:

- Strafbepalingen met betrekking tot computercriminaliteit in enge zin: computergegevens en – systemen als doelwit.
  - Bijvoorbeeld computervredesbreuk.
- Aangepaste en nieuwe strafbepalingen waarbij computers/ICT een hulpmiddel zijn.
  - Bijvoorbeeld virtuele kinderpornografie
- Gebruik van ‘oude’ bestaande bepalingen
  - Bijvoorbeeld diefstal van virtuele objecten (zie Runescape-arrest)

### **Vóór de eerste Wet Computercriminaliteit**

Voordat de eerste Wet Computercriminaliteit ontstond, werd er veel gediscussieerd over de wetgeving, waarbij de vraag speelde of het wel nodig was om nieuwe wetgeving te maken. Het ging toen voornamelijk om vermogensdelicten. Het bestanddeel ‘goed’ is ook heel belangrijk; de vraag hierbij is in hoeverre computergegevens een goed zijn.

In het elektriciteitsarrest werd bepaald dat gratis elektriciteit van een ander gebruiken hetzelfde is als het wegnemen van een goed. De Hoge Raad somde eigenschappen van elektriciteit op en keek wat het doel is van de wetsbepaling en trok daaruit de conclusie dat elektriciteit een goed is.

### **Totstandkoming Wet Computercriminaliteit (1993)**

Er ontstond de behoefte aan nieuwe strafbepalingen. Men vroeg zich af of ze het zouden redden met de al bestaande klassieke bepalingen.

De voorstanders van de bewering dat computergegevens een goed zijn deden een beroep op het elektriciteitsarrest en op het advies van Vellinga-Schootstra, die benoemde dat er geen verschil zat in het wegnemen van fysieke informatie en het ongevoegd kopiëren van gegevens.

De tegenstanders zeiden dat er een probleem was met de legaliteit van de bewering dat computergegevens een goed zijn en dat mensen beschikkingsmacht kunnen hebben over gegevens en dat door gegevens te kopiëren de ander de beschikkingsmacht niet verliest. Verder hadden ze een principieel argument, namelijk de ‘free flow of information’ (art. 10 EVRM).

In de Wet Computercriminaliteit (1993) stond uiteindelijk dat gegevens geen goed zijn en de Hoge Raad volgde dit.

### **Computercriminaliteit in enge zin**

Computercriminaliteit in enge zin:

- Het zich onrechtmatig verschaffen van computergegevens
- computervredesbreuk.
- Een **valse sleutel** gebruiken (het onrechtmatig gebruik van inloggegevens van een ander)
- Onrechtmatige onderschepping van gegevens → aftappen en opnemen
- Door middel van spyware kunnen je gegevens opgenomen worden en je gegevens kunnen makkelijk onderschept worden bij het gebruik van open Wi-Fi-netwerken.
- Het onrechtmatig verstoren van gegevens ex art. 350a Sr

- Beschadiging van hardware
- Het onrechtmatig verstoren van computersystemen
  - Toegang belemmeren ex art. 138b Sr (komt vaak voor). In lid 2 staat een strafverzwaringsgrond.

### **Computercriminaliteit in ruime zin**

Computercriminaliteit in ruime zin is een middel om tot een bepaald doel te komen. Een voorbeeld van een specifieke bepaling, gelet op technologische ontwikkelingen, is de strafbepaling van kinderpornografie ex art. 240b Sr. De woorden 'schijnbaar betrokken' en 'toegang verschaffen' kunnen ruim opgevat worden. 'Schijnbaar betrokken' ziet op virtuele kinderpornografie. Hierbij worden geen echte kinderen gebruikt, maar virtuele die niet van echte te onderscheiden zijn.

Tegenwoordig heb je ook **lokpubers** die net doen of ze jonger zijn dan 16 jaar. Dit is op zichzelf niet strafbaar. Het wordt dit wel in de nieuwe wet, dit komt dan te staan in art. 248e Sr. De derde Wet Computercriminaliteit moet nog door de Eerste Kamer. Er staat veel in over strafrechtelijke bevoegdheden. Verder is bijvoorbeeld het voorhanden hebben van gegevens die een ander gekregen heeft door te hacken nu nog niet strafbaar, maar zal dit in de nieuwe wet wel zijn. De nieuwe wet zal vooral zorgen voor verdere versterking van de bescherming van gegevens.

## **HC 7, 4-12-2018, strafvordering en IT**

### **Inleiding strafvordering-opsporingsonderzoek**

De kernbronnen van het opsporingsonderzoek zijn:

- Wetboek van Strafvordering (Sv)
- Bijzondere wetten: Opiumwet, WWM, WED
- Het internationale kader
- Jurisprudentie

### **Het wettelijke kader**

Art. 1 Sv staat centraal → legaliteitsbeginsel.

“Strafvordering heeft alleen plaats op de wijze bij de wet voorzien.”

Het begrip strafvordering is het geheel van regels betreffende de opsporing. Wie er mag vervolgen is ook opgenomen in het Wetboek van Strafvordering. De definitie van opsporing staat in art. 132a Sv.

Strafvorderlijke beslissingen zijn waar het onderzoek toe kan leiden

### **Opsporing**

Aanwijzingen voor terrorisme zijn voldoende voor het verkrijgen van bevoegdheden op het gebied van opsporing. Wanneer er sprake is van een anonieme tip moet er voldoende verdenking zijn voordat er stappen mogen worden genomen. Zie hiervoor art. 3 Politiewet en art. 141 Sv.

Art. 1 Sv is geen uitputtende regeling.

Het uitgangspunt van de wetgever is dat de persoon die is belast met opsporing in beginsel alles mag doen wat nodig is voor opsporing. Als het geen inbreuk maakt op een grondrecht, hoeft het niet geregeld te worden. Inmenging eist een grondslag in het nationale recht.

Dit recht moet toegankelijk zijn, eventueel met behulp van een deskundige.

De inbreuk moet voorzienbaar zijn, wat inhoudt dat de burger het moet kunnen weten.

In het kader van waarborgen moet de regeling des te specifiekere zijn bij een meer ingrijpende inbreuk op de privacy.

### **Grens en grenscriterium**

Er is sprake van een meer dan beperkte inbreuk op de privacy wanneer er min of meer een compleet beeld is verkregen van bepaalde aspecten van iemands privéleven → **materieel criterium**.

Een voorbeeld: als je een drone inzet in het kader van toezicht of opsporing, is de vraag of art. 3 Politiewet dan voldoende grondslag bevat en of er sprake is van meer dan een beperkte inbreuk.

Een **stelselmatige observatie** betreft een meer dan beperkte inbreuk op de privacy, waarbij dus aan de voorwaarden van art. 126g Sv is voldaan. Een niet-stelselmatige inbreuk is een beperkte inbreuk en kan

dit in beginsel gebaseerd worden op art. 3 Politiewet 2012. Stelselmatige observatie mag alleen bij misdrijven worden ingezet en voor een bepaalde duur. Bij het bepalen of een observatie stelselmatig is, moet er gekeken worden naar de duur, de plaats en de intensiteit van de observatie. Verder moet er gekeken worden naar of er gebruik wordt gemaakt van een technisch hulpmiddel.

Niet iedere inzet van een drone behoeft een wettelijke grondslag, omdat er verschillende drones zijn en ze voor verschillende doeleinden kunnen worden gebruikt.

Het EHRM geeft de voorkeur aan toetsing vooraf door een onafhankelijke autoriteit. In Nederland geldt geen eis van toestemming vooraf. Wel is compensatie achteraf mogelijk.

De wettelijke basis voor het onderzoek aan inbeslaggenomen voorwerpen door opsporingsambtenaren is gelegen in het samenstel van de bepalingen waarop de bevoegdheid tot inbeslagneming is gebaseerd (Hoge Raad).

Hof Amsterdam, ECLI:NL:GHAMS:2018:3384 geeft nog een recente toepassing aan de door de Hoge Raad in 2017 uitgezette lijn ten aanzien van het onderzoek naar smartphones.

### **Wet computercriminaliteit III**

Per 1 januari 2019 wordt het arsenaal opsporingsbevoegdheden uitgebreid.

## **HC 8, 7-12-2018, Intellectueel eigendomsrecht (deel 1)**

Wij leven in een informatiemaatschappij. Bij nieuwe ontwikkelingen komen belangen in het geding en moeten er regels worden opgesteld. Nieuwe technieken kunnen leiden tot vernieuwing van al bestaande regels. Op het moment dat we gingen digitaliseren moesten er nieuwe regels worden gemaakt. Verder vergt het dat we internationale betrekkingen hebben.

IE: intellectuele eigendom, ook wel IP (intellectual property) genoemd.

De regels roepen iets in het leven, namelijk subjectieve rechten (zoals auteursrecht en databankenrecht). Omdat het zo internationaal is moet men bij overeenkomsten de rechten van andere landen ook in acht nemen. De uitzondering hierop is de **uitputtingsregel**.

### **De waarde van een IE-recht**

Als je een IE-recht hebt, dan kun je dat zelf exploiteren of je kan licenties vrijgeven. Als je het recht niet meer wilt, kun je het overdragen. De waarde is zelf vast te stellen.

Een **licentie** is de toestemming om iets waarop een IE-recht rust te gebruiken en te exploiteren. In een licentieovereenkomst kunnen voorwaarden worden opgelegd om het gebruik in te perken. Licentie is in beginsel vormvrij, behalve als het gaat om een exclusieve licentie, zie hiervoor art. 2 lid 3 Aw.

Een IE-recht is een vermogensrecht. Het kan alleen bij akte worden overgedragen en wanneer het recht eenmaal is overgedragen, dan blijft het overgedragen en is ook alles overgedragen. De uitzondering hierop is een persoonlijkheidsrecht.

### **IE-rechten**

Er zijn verschillende soorten IE-rechten en de meest voorkomende is het auteursrecht. Naburige rechten zijn verwant aan het auteursrecht.

In de praktijk komen er verschillende problemen bij het auteursrecht kijken, zoals de vraag aan wie de rechten toekomen en welke delen van het werk beschermd zijn.

### **Conclusie**

Intellectueel eigendomsrecht is een vorm van internationale normering van concurrentie. Het heeft economische waarde, is juridisch lastig te handhaven en heeft een monopolistenpositie ten aanzien van een bepaald geestelijk product of onderscheidingsteken.

## Het auteursrecht

Het moet gaan om een maker die een werk heeft gemaakt dat openbaar is en te verveelvoudigen is. Het werk dat beschermd wordt moet **voldoende origineel** zijn. Uit de rechtspraak volgt dat het werk waarneembaar, oorspronkelijk en niet puur technisch moet zijn. De maker krijgt het auteursrecht. Het auteursrecht houdt exclusiviteit op **verveelvoudigen** en **openbaar maken** in. Dit zijn exploitatierechten. Van oorsprong is het een vrij Nederlands recht, maar Europa wilde bestaande nationale wetten harmoniseren met richtlijnen. Sommige delen van het auteursrecht zijn al geharmoniseerd, zoals het begrip ‘werk’ (Infopaq I-arrest). De terminologie in het Europese recht verschilt van de Nederlandse. In Lancôme/Kecofa is samengevat wat een werk inhoudt. In het Endstra tapes-arrest is bepaald dat er **creatieve keuzes** moeten zijn gemaakt. Bescherming geldt vanaf het moment dat het werk er is.

## Auteursrechten op software

Uit Nederlandse vaste rechtspraak volgt dat auteursrechten op software relatief snel worden aangenomen. Het moet wel voldoende origineel zijn. In het BSA-arrest 2010 is bepaald dat GUI niet valt onder de softwarerichtlijn. In het SAS/Worldprogramming-arrest 2010 is bepaald dat er geen bescherming is voor functionaliteit, indeling van gegevens en programmeertaal. In het **UsedSoft-arrest** is bepaald dat er een wettelijke licentie op het gebruik van tweedehandssoftware rust, zelfs voor software zonder drager.

## Inbreuk op het auteursrecht

Wanneer er gebruik wordt gemaakt van een werk zonder de toestemming van de maker, behalve wanneer er geen toestemming vereist is vanwege een uitzonderingsgrond, is er sprake van een inbreuk op het auteursrecht. **Uitputting** is een van die uitzonderingen; dit is een beperking van het openbaarmakingsrecht. Wanneer een exemplaar van een werk eenmaal rechtsgeldig in het verkeer is gebracht, dan kan de rechthebbende zich daar niet meer tegen verzetten (denk aan een boek of cd). Dit werkt niet voor niet-materiele zaken als MP3's of films via de ether, want dit zijn geen exemplaren. In het UsedSoft-arrest is hierover bepaald dat rechtmatige gebruikers een wettelijke licentie tot gebruik hebben, zelfs als er geen sprake is van een exemplaar, maar van een niet-materiële download. Uitputting geldt dus ook voor software! Downloaden mag alleen als er toestemming is gegeven door de maker en wanneer het alleen voor privégebruik is (ACI Adam BV/stichting de Thuiskopie).

## Linken

In het **Svensson-arrest** is bepaald dat linken naar content dat zonder toestemming van de rechthebbende is geplaatst en dat een **‘nieuw publiek’** bereikt, een vorm van openbaarmaking is. Dit standpunt wordt nog verder uitgewerkt in het GS Media-arrest en het Filmspeler-arrest. Het begrip ‘linken’ wordt ruim uitgelegd.

## Persoonlijkheidsrechten

**Persoonlijkheidsrechten** zijn morele rechten die zelfs na overdracht van de auteursrechten bij de maker blijven (o.a. het recht op naamsvermelding).

## Databankenrecht

Data bestaat uit gegevens en informatie uit gegevens met een betekenis/waarde. Kennis is datgene wat je in staat stelt om van data informatie te maken. Databanken is een manier om informatie op een geordende en gestructureerde manier in een systeem te zetten, zodat dit op elk moment opgevraagd kan worden. Een **databank** is een digitaal opgeslagen archief dat is ingericht met het oog op flexibele raadpleging en gebruik. Het beschermt de inzet van de persoon die het in het systeem heeft gezet. De definitie staat in art. 1 lid 1 sub a Dw. Een databank kan originele werken bevatten en de databank wordt automatisch beschermd door de databankenwet. Het kan ook zo origineel zijn dat het toch beschermd wordt via het auteursrecht. De bronnen voor het databankenrecht zijn de **Richtlijn 96/9/EG** van het Europees parlement en de **Databankenwet**.

## William Hill/BHB

Een belangrijk arrest is William Hill/BHB: “Substantiële investering moet betrekking hebben op de verkrijging, de controle of de presentatie van de databank en niet op het maken van de inhoud ervan.”

Als de twee exploitatierechten van de databank van de producent zonder toestemming worden gebruikt, is er sprake van een inbreuk. Volgens het Hof: “Hergebruik kan ook indirect, via andere bronnen en het dient substantieel van aard te zijn. Dit moet bekeken worden aan de hand van de grootte van de investering van het geheel.”

## Hoorcollege 9, 11 december 2018, Intellectueel eigendomsrecht (deel2)

### De functies van het merk

Een merk heeft een bepaalde functie en waarde.

Het Hof van Justitie heeft die functies (**functieleer**) een keer benoemd; als er afbreuk aan wordt gedaan is dit een inbreuk op het merkenrecht. Een merk wordt geplaatst op waarden of diensten oftewel stoffelijke producten of een stukje dienstverlening. Het hof zegt dat dit niet zomaar aangetast mag worden.

### Merkenrecht

Het merkenrecht ligt op onderscheidingstekens voor **waren** en/of **diensten**. Die worden als je gaat deponeren, onderverdeeld in veel verschillende klassen. De deposant, de toekomstige merkhouder, heeft het recht. Er zijn drie verschillende rechtssystemen op basis waarvan wij tot merkregistratie kunnen komen: Benelux, EU en internationaal. De meeste registers hebben dezelfde indeling van waarden en diensten. Een uitzondering hierop is China. Daar is het veel moeilijker om een merk te vestigen.

### Vereisten aan een merk

Het begint allemaal met een **depot**. Wie het eerst komt, wie het eerst maalt. Een ander vereiste is dat het merk een voldoende onderscheidend vermogen moet hebben om een merk te kunnen zijn. Het moet te identificeren zijn tot waar het van afkomstig is. Verder mag het niet beschrijvend zijn en er mag ook geen verwarring worden veroorzaakt met andere merken.

### Relevantie van merkenrecht in het IT-Recht

Merken zijn territoriaal begrensd (geregistreerd voor een bepaald gebied). Door IT en het internet is de wereld kleiner geworden, waardoor merkinbreuken op de loer liggen, bijvoorbeeld als een Nederlandse partij een Europees merk aanvraagt dat blijkt te lijken op een Portugees merk.

### Veel verschillende soorten merken

De meest voorkomende merken zijn woordmerken, beeldmerken, namen en logo's. De Coca-Cola fles is bijvoorbeeld een vormmerk.

### Twee categorieën merken

Er zijn twee categorieën merken: individuele en collectieve. **Individuele merken** zijn de meest voorkomende merken. Ze worden gebruikt om commerciële producten en diensten te verkopen. **Collectieve merken** zijn merken met een handleiding. Iedereen die voldoet aan de voorwaarden mag onderdeel zijn van dat keurmerk.

Pas op voor individuele keurmerken.

### Drie regimes voor Nederland

**BVIE:** opvolger Benelux Merkenwet en geharmoniseerd met de Merkenrichtlijn.

**Uniemerkenverordening:** met één merkdepot heb je bescherming in de hele EU.

**Overeenkomst van Madrid:** hier doen ongeveer 80 landen aan mee (het minst belangrijke regime).

Bij het Beneluxdepot is de depotdatum leidend. De oppositieperiode is twee maanden vanaf de publicatie. Het merk is tien jaar geldig vanaf depotdatum. Het uniemerkdepot lijkt er erg op, alleen is daarbij de oppositieperiode drie maanden vanaf de publicatie.

### Einde merk

Een merk kan beëindigd worden:

- Door geen verlenging aan te vragen na looptijd van 10 jaar;
- Door vrijwillige doorhaling;

- Door verwatering tot soortnaam;
- Bij geen normaal gebruik gedurende vijf jaar;
- Als het merk het publiek misleidt.

Te weinig onderscheidende of te veel beschrijvende tekens kunnen door veelvuldig gebruik en marketing een merk worden, ook wel **inburgering** genoemd. Een merk kan ook de onderscheidingskracht verliezen, dit heet **verwatering** (hagelslag is hier een voorbeeld van).

### **Inbreuk op een merkenrecht**

In art. 2.20 lid 1 BVIE/art.9 lid 1 Verordening staan inbreuken op een merkenrecht opgesomd. Als dingen identiek aan elkaar zijn, dan speelt verwarring geen rol. Als er echter alleen gelijkenissen zijn, dan zou er verwarring kunnen ontstaan. Het gaat om het risico. In sommige gevallen moet de merkhouders een vergelijkbaar teken dulden. In het Interflora-arrest is bepaald dat er sprake kan zijn van een geldige reden voor het gebruik van een ander merk. Het moet dan voldoen aan de volgende vier criteria:

- Het biedt een alternatief;
- Het mag geen imitaties bevatten;
- Het mag geen afbreuk of verwatering van het merk veroorzaken;
- Het mag overige functies van het merk niet aantasten.

### **Handelsnamen**

Een handelsnaam geeft geen subjectief recht; dat wil zeggen dat het geen recht aan een individu of rechtspersoon geeft om een bepaalde naam te voeren. Het is geen vermogensrecht. Het zegt wat wel en niet mag. Iedere onderneming is vrij om binnen de grenzen van de Handelsnaamwet een handelsnaam te dragen. Het is verboden om verwarrende en misleidende handelsnamen te voeren (art. 3-5b Hnw). Een handelsnaam ontstaat niet door inschrijving bij de KvK, maar door werkelijk gebruik te maken van de handelsnaam (art. 1 Hnw). Overdracht is alleen mogelijk wanneer dit samen gaat met de overdracht van de onderneming die onder die handelsnaam wordt gedreven. In de praktijk wordt het vaak anders gedaan. In het **Mosterdmanneke-arrest** staat de Hoge Rad licenties op handelsnamen toe. Inbreuk op een handelsrecht is niet mogelijk. Men kan alleen optreden wanneer een andere partij zich niet houdt aan de Hnw.

### **Domeinnamen**

Een verwijzing naar internetadressen is in Nederland uitgegeven door SIDN. Domeinnamen zijn geen IE-rechten. Als de domeinnaam wordt gebruikt als handelsnaam, dan is het beschermd. Bij het aanvragen van domeinnamen geldt dat degene die als eerste kwam, de naam mag voeren.

### **Onrechtmatige daad**

Alles wat civielrechtelijk niet mag is een onrechtmatige daad. Hierna een leerstuk dat IE gerelateerd is. **Slaafse nabootsing** is het zodanig onrechtmatig profiteren of nabootsen van een merk, dat het nodeloze verwarring wekt bij het publiek. Hier is sprake van wanneer de nabootser heeft nagelaten alles te doen wat redelijk was om gevaar voor verwarring te voorkomen en het nagebootste product zich kan onderscheiden op de markt van de andere modellen. Slaafse nabootsing is het belangrijkste leerstuk op het gebied van IE-recht dat onder onrechtmatige daden valt.

## **HC 10, 14-12-2018, E-commerce: dienstverlener van de informatiemaatschappij**

### **Elektronische handel**

Elektronische handel bestaat uit meer dan alleen overeenkomsten. Bijvoorbeeld bij het gebruik van Google zijn veel algemene voorwaarden van toepassing. **Indirecte e-commerce:** totstandkoming via netwerken. **Directe e-commerce:** ook uitvoering via netwerken (het gebruik van Spotify). B2B/B2C valt ook onder elektronische handel.

E-commerce is geïmplementeerd in het Burgerlijk Wetboek (richtlijn elektronische handel).

De richtlijn consumentenrechten gaat over overeenkomsten op afstand en staat ook in het Burgerlijk Wetboek. De Europese verordening eIDAS ziet er op toe dat burgers in het algemeen en consumenten in het bijzonder vertrouwen kunnen hebben in hun onderlinge relaties met partijen. Hierin gaat het over

vertrouwensdiensten en de uitvoeringswet staat in art. 3:15a-c BW. De nationale wetgever heeft ook bepalingen gemaakt over e-commerce: Wet elektronisch rechtsverkeer.

### **Diensten van de informatiemaatschappij**

De definitie van diensten van de informatiemaatschappij is neergelegd in art. 3:15d lid 3 BW, het gaat hier om:

- elke dienst
- gewoonlijk tegen vergoeding
- op afstand
- op individueel verzoek

#### *Elke dienst*

Het belang van diensten zit hem in de vrije vestiging in Europa. Het geeft informatieplichten bijvoorbeeld d.m.v. reclame en overeenkomsten. Verder worden tussenpersonen aansprakelijk gesteld. De definitie staat in art. 3:15d lid 3 BW: elke dienst → Platforms die invloed uitoefenen op juridische relatie tussen partijen. Een voorbeeld hiervan is de Uber test: De hoofdvraag is hier of de taxidienst onlosmakelijk verbonden is met de app. Als dit los van elkaar staat, dan valt de taximaatschappij buiten de eIDAS-wetgeving. Is de Uber-app nodig voor het maken van de markt? Ja. Heeft Uber beslissende invloed op de vervoersdienst? Ja. Hieruit blijkt dat de app en taxidienst onlosmakelijk met elkaar verbonden zijn. Een ander voorbeeld is Airbnb. Airbnb oefent wel enige, maar niet beslissende invloed uit. De huurprijs stellen ze bijvoorbeeld niet vast.

#### *Gewoonlijk tegen vergoeding*

Er bestaan ook gratis diensten zoals Twitter en Instagram, maar eigenlijk betaal je bij die platforms met persoonsgegevens.

#### *Op afstand*

Het moet langs de elektronische weg en op afstand worden verricht, ook mogen de partijen zich niet op dezelfde plaats bevinden.

#### *Op individueel verzoek*

Het moet niet opgedrongen worden, maar uit eigen beweging van de afnemer plaatsvinden. De afnemers moeten naar de dienstverlener toegaan.

### **ISP's en reclame**

Virale filmpjes

Reclame moet herkenbaar zijn als reclame. Het is verboden om net te doen alsof het geen reclame is. De identiteit van de persoon die achter de reclame zit moet ook duidelijk zijn. Online reclame wordt inhoudelijk beoordeeld naar mate van invloed en aanprijzing → **dubbele maatstaf**. Een voorbeeld is de gebruikerswaardering. Mate van invloed: er is sprake van reclame wanneer de eigenaar er invloed op heeft gehad.

### **Aansprakelijkheid tussenpersonen**

SABAM/Netlog

Afweging door het Hof:

- Een social netwerk is een hosting provider (slaat gegevens van gebruikers op)
- Een preventief filter als gevorderd gaat te ver
  - Intellectueel eigendomsrecht beschermd, maar niet absoluut (r.o. 41)
  - Ernstige aantasting vrij ondernemerschap (r.o. 46)
  - Aantasting privacy en informatievrijheid (r.o. 49-50)

Er zijn minder vergaande maatregelen mogelijk ex art. 6:196c lid 5 BW.

Bijvoorbeeld:

- Blokkade van de site



- Blokkade aanbieder van de informatie
- NAW-gegevens verschaffen

Hierbij blijft de afweging van belangen altijd noodzakelijk. **Regeling van de safe haven:** beperking aansprakelijkheid tussenpersonen. Er moet onderscheid gemaakt worden tussen acces providers, internetproviders en serviceproviders. Het hof vindt het verplichten van dit preventieve filtersysteem te ver gaan. Ook mag intermediaire dienstverleners niet de algemene verplichting worden opgelegd om onderzoek te doen naar illegale informatie, dit blijkt uit het arrest *L'Oréal/eBay*.

## HC11, 18-12-2018, elektronisch contracteren

### Totstandkoming

Een overeenkomst komt tot stand door aanbod en aanvaarding, ex art. 6:217 BW. Aanbod en aanvaarding komen voort uit een wil, ex art. 3:33 BW. Of er een overeenkomst tot stand is gekomen hangt af van de omstandigheden van het geval.

Als er geen sprake is van intellectueel eigendomsrechtbescherming, dan kan er iets geregeld worden.

### Aviation/Ryanair

Click-wrap is een hele veilige manier om gegevens te beschermen. Ryanair deed dit niet vanaf het begin en in deze uitspraak ging het erom dat ze eerst alleen onderaan de beginpagina in kleine lettertjes vermeldden dat de voorwaarden van toepassing waren en of dit genoeg was. Dit wordt browse-wrap genoemd. In de uitspraak werd bepaald dat dit niet voldoende was.

### Elektronische verklaring

De overeenkomst komt tot stand wanneer de verklaring de andere persoon heeft bereikt ex art. 3:37 lid 3 BW. Bij elektronische verklaring zoals een e-mail, moet deze dus eerst ontvangen zijn in de mailbox. Bij de totstandkoming zijn er nog een aantal specifieke regels. Een webshop moet bijvoorbeeld voorzien in fouterstel (art. 6:227c lid 1 BW), wat ook openbaar moet zijn voor de consument. Is dit niet het geval, dan is de overeenkomst vernietigbaar.

### De ontvangstbevestiging

Ook moet er een ontvangstbevestiging worden verstuurd (art. 6:227c lid 2 BW) wanneer er een bestelling is geplaatst. Dit biedt zekerheid voor de consument dat de bestelling goed tot stand is gekomen. Als dit niet (op tijd) gebeurt, dan kan de overeenkomst ontbonden worden.

### Informatieplichten

Bij informatieplichten gelden een wilsfunctie en dossierfunctie. Deze hebben vaak ontbinding als consequentie

In art. 6:227b BW staan twee bijzondere informatieplichten. De eerste is de **informatie over de wijze van contracteren**. Een bestelpagina moet duidelijk in elkaar zitten, zodat de consument dit kan begrijpen en het stappenplan kan volgen. Een voorbeeld waarbij het helder uitgelegd is dat de klant aan vervolgleveringen gebonden is, volgt uit de uitspraak *consumentenautoriteit/Postgarant*. Er moet ook een mogelijkheid zijn voor de gebruiker om fouten te verbeteren bij de bestelling. Het systeem van fouterstel van de website moet ook werken. Verder moet de dienstverlener **transparant** zijn, dat houdt in de informatie op een 'duidelijke, begrijpelijke en ondubbelzinnige wijze' verschaffen. Als de informatie over het proces van totstandkoming en de foutenverbetering niet op de juiste manier verleend wordt, maakt dit de overeenkomst vernietigbaar voor de wederpartij.

De tweede informatieplicht is **informatie over kernbedingen**. De kernbedingen zijn bedingen zonder welke de overeenkomst niet tot stand kan komen. Deze kernbedingen moeten vooraf duidelijk zijn. Wanneer deze informatieplicht geschonden wordt, kan de overeenkomst worden ontbonden, totdat de kernbedingen alsnog worden verstrekt.

### Algemene voorwaarden

Algemene voorwaarden zijn bedoeld om als contractbedingen meerdere keren in contractuele verhoudingen gebruikt te worden. Kernbedingen vallen hier niet onder. Volgens art. 6:234 BW moeten

de algemene voorwaarden toegankelijk zijn en downloadbaar. Wanneer er niet aan de algemene voorwaarden voldaan wordt, kan de overeenkomst vernietigd worden.

### **Overeenkomst op afstand**

Op een overeenkomst op afstand is de *Richtlijn consumentenrechten* van toepassing. Het gaat bij een **overeenkomst op afstand** tussen een handelaar en een consument, die op afstand wordt gesloten, via een georganiseerd systeem van verkoop of dienst. Een overeenkomst op afstand kan herroepen worden zonder opgave van redenen binnen veertien dagen, ex art. 6:230o lid 1 BW.

### **Informatieplichten bij overeenkomsten op afstand**

In art. 6:230m BW staat een opsomming van de precontractuele informatie die door de handelaar moet worden verstrekt.

### **Vorm bij online contracteren**

De hoofdregel is dat rechtshandelingen vormvrij zijn. Soms is een schriftelijk document verplicht voor het verrichten van een rechtshandeling. Het kan ook tot bewijs dienen.

## **HC 12, 21-12-2018, IT-contracteren**

### **Automatisering algemeen**

Automatisering vormt vaak de kern van een organisatie. Bij automatisering gelden verschillende regels, deze zijn vooral neergelegd in het verbintenissenrecht. De onderlinge partijafpraak is bepalend voor de rechtsverhouding. De rechtspraktijk rond deze contracten is vaak zeer complex. Er zijn vier vormen van automatisering.

### **Standaardsoftware**

De eerste vorm van automatisering is **de inhoud van standaardsoftware**. Bij de invoer van deze standaardsoftware wordt een kant-en-klaar softwareproduct aangeschaft. Het nadeel van deze standaardsoftware is dat het niet wordt aangepast op specifieke behoeften die de organisatie kan hebben. Standaardoplossingen zijn echter wel meestal de beste. Het gebruik van standaardsoftware komt het meest voor in kleinere bedrijven.

### **Maatwerksoftware**

Het schrijven van een geheel nieuw softwareproduct wordt ook wel **maatwerksoftware** genoemd. Hierbij worden de behoeften van de organisatie in kaart gebracht. Dit kost veel geld en het duurt lang. In de praktijk is er niet altijd sprake van een strikt onderscheid tussen maatwerksoftware en standaardsoftware. Standaardsoftware wordt soms ook op maat gemaakt.

### **Software ‘as a service’ (Saas)**

Wanneer de informatieverwerking uitgevoerd wordt via een netwerkverbinding is er sprake van **Software as a service**. In de praktijk wordt dit ook wel dienstverlening via de Cloud genoemd. De klant kan op afstand gebruik maken van de functionaliteit van een computerprogramma, zonder over een kopie te beschikken. Dit is mogelijk met behulp van breedbandnetwerkverbindingen. Het voordeel hiervan is dat de gebruiker geen gespecialiseerde apparatuur of personeel nodig heeft voor het onderhoud van zijn automatisering. Een nadeel is dat Saas-constructies juridisch complexe verantwoordelijkheidsverdelingen kunnen opleveren.

### **Diensten rondom automatisering**

Rondom de invoering en uitvoering van automatisering worden allerlei diensten aangeboden. **Advies** is een van die diensten. Degene die adviseert is de automatiseerder. Hierbij dient hij zich tegenover de klant als een redelijk handelend en bekwaam leverancier op te stellen (*RBC/Brinkers*). Ook de aanschaf van **hardware** kan onderdeel zijn van een automatiseringscontract. Hierop zijn alle bepalingen met betrekking tot koop van toepassing. Wanneer een organisatie hun automatisering aan een andere organisatie uitbesteden is dit **outsourcing**. Een andere dienst rondom automatisering is **onderhoud**, waar vaak een apart contract voor wordt afgesloten.