ICTRECHT
adviesbureau

ICTRECHT
IN DE PRAKTIJK

jaargang 7 nummer 3 juli 2019

Naar een definitie van het begrip 'internetrecht'

De parodie als uitzondering op de Auteurswet

Belangrijke aandachtspunten bij cross-border e-commerce

Heeft u uw juridische zaken goed geregeld?

Zeker op het gebied van ICT en privacy is dit geen eenvoudige zaak.
Voorkom juridische ICT- of privacyproblemen en laat ICTRecht u deskundig en praktisch adviseren.
Dat hoeft helemaal niet duur te zijn: naast maatwerk leveren wij standaardproducten en juridische generatoren.

ICTRecht is een flexibel en creatief juridisch adviesbureau. Wij bedienen zowel de grote als de kleine klant. Onze adviezen zijn begrijpelijk, concreet en geven blijk van technische kennis. Onze mensen zijn dan ook juridisch en technisch thuis in onze niche.

Wij kunnen u van dienst zijn met:

Juridische documenten - Juridisch advies - Juridische detachering
Trainingen - Generatoren - Boeken

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

ICTRECHT
adviesbureau

Voorwoord

Vijftien jaar alweer bestaat ons adviesbureau. Deskundig en praktisch advies over internet en recht. Eén vraag heeft ons daarbij altijd bezig gehouden: wat is internetrecht nu eigenlijk? Bestaat dat eigenlijk wel, dat rechtsgebied. In dit nummer doen wij een poging een juridisch omlijnde definitie te geven.

Wat internetrecht ook is, de relevantie van internet voor de gezondheid wordt steeds groter. Daarom in dit nummer een blik op nieuwe wetgeving rondom medische hulpmiddelen, die ook impact heeft op apps. Bij apps horen cookies en tracking, dus ook daar kijken we in dit nummer naar.

Een blik op de toekomst – nog vijftien jaar internetrecht! – kan natuurlijk niet zonder het laatste *hot topic*: de smart contracts, zichzelf regulerende afspraken zonder rechterlijke tussenkomst. Wat gaat daarmee gebeuren?

En als laatste: op 15 november vieren wij ons jubileum met een uniek congres. Komt u ook?

Directie
Steven Ras en Arnoud Engelfriet

Index

Colofon

Dit is een uitgave van ICTRecht B.V.
020 663 1941, info@ictrecht.nl.

Dit tijdschrift verschijnt vier keer per jaar. Proeftijdschrift is op aanvraag beschikbaar. Abonnementsprijs is € 135,- excl. btw per jaar (papieren editie), inclusief verzendkosten in Nederland. Voor een jaarabonnement (digitale editie) betaalt u € 67,50 excl. btw.

Aan deze uitgave werkten mee:
Arnoud Engelfriet - Algemeen directeur / Opleidingsdirecteur - a.engelfriet@ictrecht.nl
Steven Ras - Algemeen directeur - s.ras@ictrecht.nl
Bram de Vos - Juridisch adviseur - b.devos@ictrecht.nl
Linde Mensink - Juridisch adviseur - l.mensink@ictrecht.nl
Samantha van de Stouwe - Juridisch adviseur - ICTRecht Groningen - s.vandestouwe@ictrecht.nl
Tim Wokke - Juridisch adviseur - t.wokke@ictrecht.nl
Henrike Bongers - Manager learning & development ICTRecht Detachering - h.bongers@ictrecht.nl
Jorien Zwaneveld Legal Assistant - ICTRecht Groningen - j.zwaneveld@ictrecht.nl
André Kamps - Juridisch adviseur - ICTRecht Groningen - a.kamps@ictrecht.nl
Michelle Wijnant - Juridisch adviseur - m.wijnant@ictrecht.nl
Dimmen Smolders - Juridisch adviseur - d.smolders@ictrecht.nl
Tessa van Schijndel - Juridisch adviseur - t.vanschijndel@ictrecht.nl
Alisa Schurink - Opleidingscoördinator en Marketingmedewerker - a.schurink@ictrecht.nl
Britt Telleman - Office- en Legal Assistant - b.telleman@ictrecht.nl
Nicole Waaijer - Marketing adviseur - n.waaijer@ictrecht.nl
Arjan van Amsterdam - Vormgever - arjan@studiovanamsterdam.nl
Leonard Fäustle Stills & Motion - foto's ICTRecht - info@leonardfaustle.nl

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Privacy | Cloud | E-commerce | Innovatie

Naar een definitie van het begrip 'internetrecht'

Het begrip internetrecht of ict-recht is inmiddels volledig ingeburgerd, maar opmerkelijk genoeg lijkt een werkbare definitie van dit rechtsgebied nog steeds te ontbreken. Allebei betekenen ze hetzelfde: het recht voor zover dat betrekking heeft op internet. En voor de iets ruimdenkendere mensen heet het dan ict-recht, het recht rond de informatie- en communicatietechnologie in brede zin. Maar als je er wat dieper over nadenkt, dan kun je je afvragen of dit wel een echt vakgebied moet zijn. Want is 'internet' of 'ICT' wel een specifiek juridisch gebied? Waarom bestaat dat eigenlijk, internetrecht? En verdient dat het wel om een eigen rechtsgebied te zijn? Laat ik eens een poging wagen.

Feitelijke complexiteit

In de praktijk lijkt een informele definitie van internetrecht (dat ik maar even gebruik als synoniem voor cyberlaw, ict-recht, technologierecht en vergelijkbare termen) vaak neer te komen op het feit dat het zwaartepunt van de rechtsvraag zich bevindt in een internet- of ict-aspect van de zaak.[1] Inbreken in iemands computer – computervredebreuk – is dus internetrecht, omdat de kwalificatie van dit feit ict-specifieke aspecten kent die doorslaggevend zijn voor de zaak.[2] Iemands hersens inslaan met een laptop is dat niet.

Deze wijze van categoriseren is goed werkbaar, maar kent wel een fundamentele zwakte. Zij komt namelijk neer op een subjectieve inschatting van de ict-specificiteit, oftewel hoe ingewikkeld het is om de ict-georienteerde feiten juridisch te duiden of het best passende wetsartikel te vinden. Het is zeker zo dat deze duiding vaak complex is en specialistische kennis vereist, maar is dat rechtvaardiging genoeg om van een eigen rechtsgebied te spreken? Neem *ransomware*, een misdrijf waarbij iemands bestanden via encryptie in gijzeling worden genomen en de sleutel na betaling van enkele honderden euro's in bitcoins wordt verstrekt.[3] Dit is in de kern niet anders dan een andere gijzeling – ik heb je paard, laat 300 euro achter in de prullenbak achter het standbeeld – met een technisch verbeterde uitvoering en meer bescherming voor de ontvoerder. Waarom noemen we dat dan toch cybercrime, internetcriminaliteit? Waarom is dit meer dan gewoon strafrecht met een toevallige technische slimme delictsuitvoering?

De cynische samenvatting van bovenstaande is dat een casus als 'internetrecht' wordt gekwalificeerd wanneer deze technisch te moeilijk is voor de beoefenaars van een der klassieke rechtsgebieden. Oftewel, een kwestie is internetrecht omdat zij feitelijke of kwalificatievragen oproept die de gemiddelde beoefenaar (nog) niet kan wegen. Vanuit de klassieke rechtsgebieden is dit een logisch standpunt: de feitelijke complexiteit van een zaak moet geen reden zijn om haar juridisch anders te kwalificeren.

Het maatschappelijk belang

Een andere tegenwerping tegen de kwalificatie van internetrecht als vakgebied is de aparte maatschappe-

1 Vergelijk de uitgebreide pogingen van Fleur Bolhaar et al, 'Wat is internetrecht?' TvIR 2014-6, p. 183.
2 Vergelijk ECLI:NL:RBMNE:2019:1151 waarin de vraag centraal stond of voor als agent privé-doeleinden in een politiedatabase kijken telt als computervredebreuk of 'slechts' als plichtsverzuim.
3 Art. 350 lid 1 Strafrecht.

lijke relevantie. Deze tegenwerping wordt vaak ondersteund met de term 'paardenrecht'.[4] Dat zit zo. Natuurlijk geldt de wet ook bij dingen die paarden betreffen (aansprakelijkheid voor een op hol geslagen paard, of conformiteit bij een gekocht paard). En natuurlijk zijn er juristen gespecialiseerd in paardenrecht – pardon, hippisch recht – en zijn er zeker rechtsvragen die complexer worden wanneer het paard centraal staat, maar daarmee spreken we nog niet van paardenrecht. Dat is niet belangrijk genoeg in de praktijk, ook al zijn er advocaten die in dat gebied werken.

Is internetrecht een vorm van paardenrecht? Niet volgens onze eigen internetrechtprofessor Arno Lodder. Internet verdient zijn eigen rechtsgebied, want internet past in het rijtje voedsel en drinken, een eerste levensbehoefte waar vrijwel niemand meer zonder kan.[5] Dat maakt het belangrijker dan paarden, en fundamenteler dan regels over het slopen van sloten. Nog verder gaat de Amerikaanse jurist Lawrence Lessig. Hij ziet het internet als een fundamentele vernieuwing in de maatschappij, zo groot en zo belangrijk dat ook het recht erdoor verandert.[6] De software en infrastructuur van internet veranderen onze normen en waarden, en die liggen ten grondslag aan het recht. Daarom is internetrecht meer dan alleen de regeltjes over internet, er gebeurt iets heel fundamenteels waar het recht wat van moet vinden. "*[M]ore than law alone enables legal values, and law alone cannot guarantee them.*"

Het informatierecht als startpunt

Vanuit een volkomen andere visie vertrok Egbert Dommering in zijn boek *Informatierecht*[7] in een poging het informatierecht te definiëren als rechtsgebied. Dit gebied bestudeert, aldus Dommering, de juridische beginselen die de randvoorwaarden vormen voor de informatiesamenleving. De informatiesamenleving is een samenleving waarin informatie oftewel kennis een van de belangrijkste productiefactoren is. Wij leven momenteel in een dergelijke samenleving dankzij het internet, vandaar dat velen informatierecht en internetrecht op één lijn stellen. Informatierecht is echter fundamenteler.

In de informatiesamenleving signaleerde Dommering drie grondrechten die elkaar beïnvloeden: de informatievrijheid, de privacy en het auteursrecht/IE. Bij informatievrijheid gaat het om informatie mogen vergaren en verspreiden, terwijl privacy en auteursrecht juist proberen verspreiding aan banden te leggen om andere belangen te verdedigen. Privacy dient dan het belang van de burger, en auteursrecht het belang van de informatieproducent. Ik denk dat er nog een vierde grondrecht bij deze drie hoort: de ondernemersvrijheid, het grondrecht om producten en diensten aan te bieden tegen betaling (of gratis, tegen advertenties dus). Internet is immers niet zomaar een netwerk, het is uiteindelijk een kluwen aan bedrijven en instellingen die er dingen mee doen en vaak daarmee geld willen verdienen.

Van een casus op het gebied van informatierecht is dan sprake wanneer deze aan één of meer van deze grond-

4 F. H. Easterbrook, 'Cyberspace and the Law of the Horse', U. Chi. Legal F. (1996): 207.

5 A. R. Lodder, 'Recht rond cyberwar, internet van dingen en andere internet (on)gemakken: de tien geboden van het internetrecht', oratie Amsterdam VU 2012. http://dare.ubvu.vu.nl/handle/1871/38020

6 L. Lessig, 'The law of the horse: What cyberlaw might teach', Harvard law review 113.2 (1999): 501-549.

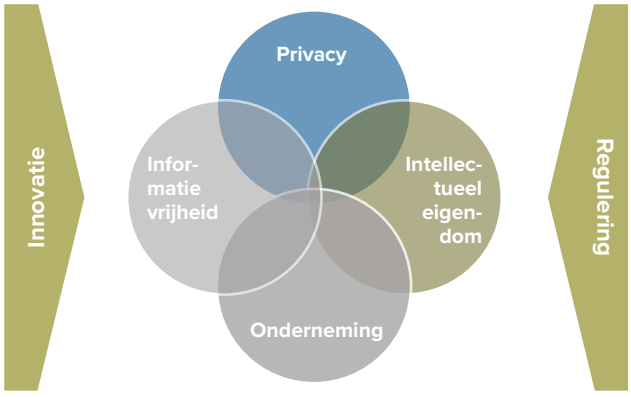
7 Otto Cramwinckel 2000.

rechten raakt, en met name wanneer sprake is van een botsing tussen twee of meer grondrechten. Het al dan niet moeten blokkeren van de beruchte *Pirate Bay* met verwijzingen naar illegaal te downloaden materiaal, is een klassieker in het informatierecht: auteursrecht versus informatievrijheid. Of, praktischer: auteursrecht versus ondernemingsvrijheid.

Internetrecht: spanningsveld tussen grondrechten

Die vier grondrechten leveren een spanningsveld op waar je zo ongeveer elk probleem binnen het internetrecht in kunt plaatsen als botsingen van grondrechten. Informatievrijheid kan botsen met de ondernemersvrijheid, en dat uit zich bijvoorbeeld in het onderwerp netneutraliteit. De gebruiker wil toegang tot alles, de ondernemer wil veel verdienen en dat gaat beter met tolpoortjes en dure hogesnelheidslijnen. Wat is dan rechtens? Hoe zit het met spontaan wijzigende algemene voorwaarden: ik zit op een platform, de voorwaarden veranderen en dan moet ik maar ophoepelen als me dat niet bevalt. Is dát wel fair? Of wat te denken van privacy versus ondernemersvrijheid: welke persoonsgegevens mag een ondernemer opeisen om een gratis dienst te leveren, en wat moet hij daarmee mogen kunnen doen? En zo kan ik nog wel even doorgaan.

Naast deze vier op elkaar inwerkende grondrechten, zijn er nog twee aspecten. Allereerst is daar de behoefte aan regulering om zo grip te krijgen op het internet. Dit verstoort de balans tussen die vier grondrechten en levert daarmee nieuwe rechtsvragen op. Ten tweede is daar de technologische vooruitgang: internet en ict kenmerkt zich door een stormachtige opvolging van ontwikkelingen. Ook dit geeft vele nieuwe rechtsvragen. Ik vat dit samen in onderstaand schema.



Het internetrecht definieer ik dan als dan het rechtsgebied dat zich richt op botsingen tussen deze grondrechten die zijn ingegeven door een nieuwe innovatie of nieuwe regulering op informatie(technologie-)gebied.

Kenmerkend (en volgens mij nieuw) aan deze definitie is dat zij focust op vernieuwing. Deze zwakte van het klassieke internetrecht – de scope verschuift steeds – is denk ik wel kenmerkend voor het soort rechtsvraag dat we in dit gebied kennen. Dit is namelijk een uniek aspect aan internetrecht: door de tijd heen, met name wanneer de technische aspecten voldoende breed begrepen worden, wordt een casus minder snel als internetrecht gekwalificeerd. Een aankoop bij een webwinkel is anno 2019 een standaardcasus in het consumentenrecht, bijvoorbeeld. Eind jaren negentig kon men menig juridisch congres vullen met internetrechtelijke vragen over dit onderwerp.

Het internetrecht is daarmee inderdaad een functioneel rechtsgebied[8], met eigen recht van bestaan omdat juist deze soort botsingen belangwekkend zijn voor de maatschappij. Haar rechtsvragen focussen op de botsingen, de veranderingen die internet met zich meebrengen. Dat is niet slechts een 'wachtkamer' voor andere rechtsgebieden. Dit rechtsgebied verdient haar eigen positie binnen de rechtswetenschappen vanwege de unieke en vernieuwende rol die internet in onze maatschappij speelt.

8 Zie ook M. Paapst, 'Is het internetrecht een eigen rechtsgebied?', http://mathieu.paapst.nl/?p=238

SAVE THE DATE

THE FUTURE IS LEGAL

15 UNIEKE LEZINGEN OVER DE TOEKOMST
VAN TECHNOLOGIE EN RECHT

VRIJDAG 15 NOVEMBER
09:00 TOT 17:00 UUR
SPOORWEGMUSEUM UTRECHT

THEFUTUREISLEGAL.NL

ICTRECHT

15 jaar

THE FUTURE IS LEGAL
Het congres waarmee we
15 jaar ICTRecht vieren

AI • PLATFORMS • FAKE NEWS • SLIMME AUTO'S • GEZONDHEID • BURGERRECHTEN • REGULERING

Bram de Vos
Juridisch adviseur

Wet- en regelgeving

Cybersecurity verordening
Op 12 maart 2019 heeft het Europees Parlement ingestemd met een voorstel voor een nieuwe Europese Cybersecurity verordening. Onder de verordening wordt het huidige Agentschap van de Europese Unie voor Netwerk- en Informatiebeveiliging (ENISA) omgevormd tot een permanent Europees agentschap. Daarmee krijgt het agentschap een permanent mandaat en een duidelijkere rol als het gaat om cybersecurity. Daarnaast introduceert de verordening een nieuw mechanisme voor het opzetten van certificeringsregels voor ICT-producten en diensten. De Europese Unie hoopt dat hiermee de veiligheid van dergelijke producten en diensten kan worden gewaarborgd en ook het vertrouwen daarin kan worden versterkt.

https://bit.ly/2u4DIm5

Boetebeleidsregels Autoriteit Persoonsgegevens 2019
Op 14 maart 2019 heeft de Autoriteit Persoonsgegevens (AP) nieuwe boetebeleidsregels gepubliceerd. Eerder heeft het European Data Protection Board (een Europees samenwerkingsverband van privacytoezichthouders) al richtsnoeren vastgesteld voor het opleggen van bestuurlijke boetes onder de AVG. In deze richtsnoeren zijn echter geen berekeningsmethoden vastgelegd. Om die reden heeft de AP nu eigen beleidsregels vastgesteld, waarin wordt uitgewerkt hoe de hoogte van de boetes in Nederland wordt bepaald. In de beleidsregels wordt (net als in de oude beleidsregels) onderscheid gemaakt tussen een aantal boetecategorieën. Voor iedere categorie geldt een eigen bandbreedte met een minimum- en maximumbedrag. Op basis hiervan wordt een basisboete vastgesteld, die aan de hand van een aantal factoren (zoals de aard, ernst en duur van de overtreding) nog kan worden verhoogd of juist verlaagd.

https://bit.ly/2HMHZ63

Richtlijn inzake auteursrechten in de digitale eengemaakte markt
Op 26 maart 2019 heeft het Europees Parlement ingestemd met het voorstel voor een nieuwe Europese Auteursrechtrichtlijn. Deze richtlijn moet het bestaande auteursrechtenkader moderniseren, zodat dit beter aansluit op de digitale samenleving van vandaag. De richtlijn voorziet onder andere in regels om de grensoverschrijdende toegang tot online diensten te verbeteren. Ook worden er nieuwe uitzonderingen op het auteursrecht geïntroduceerd, onder andere voor tekst- en datamining en online-onderwijsactiviteiten. Op de richtlijn is tijdens de wetgevingsprocedure vanuit verschillende hoeken kritiek geuit. Deze kritiek heeft onder meer te maken met het veelbesproken “artikel 13” (in de uiteindelijke versie van de richtlijn artikel 17). Aanbieders van onlinediensten voor het delen van content (denk aan platforms als YouTube) moeten “volgens strenge sectorale normen” maatregelen nemen om te voorkomen dat er via hun dienst auteursrechtinbreuken worden gepleegd. Indien er niet voldoende maatregelen zijn genomen om inbreukmakend materiaal te blokkeren, kan de dienstverlener zelf aansprakelijk worden gesteld. Er is vooralsnog veel onduidelijkheid over het toepassingsbereik van de regeling en de maatregelen die van de dienstverleners mogen worden verwacht.

https://bit.ly/2HHRyUg

New deal voor de consument
Op 2 april 2019 hebben het Europees Parlement en de Raad een voorlopig akkoord bereikt over het aanscherpen en beter handhaven van regels om consumenten te beschermen. De “*new deal*” bestaat uit twee onderdelen. Allereerst worden er wijzigingen voorgesteld in de Richtlijn oneerlijke bedingen in consumentenovereenkomsten, de Richtlijn bescherming van de consument inzake prijsaanduidingen, de Richtlijn oneerlijke handelspraktijken en de Richtlijn consumentenrech-

ten. Ten tweede bevat de *new deal* een voorstel voor een nieuwe verordening inzake de afwikkeling van massaclaims. De new deal moet zorgen voor meer transparantie bij online consumentenaankopen, doeltreffende sancties en duidelijke regels voor de aanpak van kwaliteitsverschillen bij producten die in de EU worden aangeboden.

https://bit.ly/2KlQcPT

Verordening versterking van de beveiliging van identiteitskaarten en verblijfsdocumenten
Op 4 april 2019 heeft het Europees Parlement ingestemd met een verordening die de veiligheid van identiteitskaarten en andere verblijfsdocumenten binnen de Europese Unie moet versterken. Verschillende lidstaten maken op dit moment nog gebruik van identiteitsdocumenten met zwakke beveiligingskenmerken, die bijvoorbeeld nog op papier worden uitgegeven. Dergelijke documenten kunnen makkelijk worden vervalst en door terroristen of andere criminelen worden misbruikt. Met de nieuwe verordening komt er een uniform kader voor de minimale beveiligingskenmerken waaraan identiteitsbewijzen en andere verblijfsdocumenten moeten voldoen. Zo wordt het verplicht om bij de aanvraag van een identiteitskaart twee vingerafdrukken af te staan. Deze worden (samen met de pasfoto) opgeslagen op een contactloze chip.

https://bit.ly/2uU48YI

Ethische richtsnoeren voor betrouwbare AI
Op 8 april 2019 heeft de Europese Commissie ethische richtsnoeren voor betrouwbare AI gepubliceerd. Ondanks de potentiële voordelen van het gebruik van AI, gaan hiermee ook ingewikkelde juridische en ethische vragen gepaard. In de nieuwe richtsnoeren worden zeven criteria geformuleerd waaraan betrouwbare AI zouden moeten voldoen. Deze criteria variëren van "transparantie" tot "veiligheid" en "diversiteit en non-discriminatie". De richtsnoeren bevatten ook evaluatielijsten aan de hand waarvan een AI kan worden beoordeeld. In de zomer van 2019 wil de Europese Commissie een grootschalig proefproject starten om de richtsnoeren in de praktijk te testen.

https://bit.ly/2VtXl37

Oprichting Europees Strafregisterinformatiesysteem
Op 9 april heeft de Raad zijn definitieve goedkeuring gegeven voor de introductie van een nieuw Europees Strafregisterinformatiesysteem (ECRIS TCN). Het systeem bevat identiteitsgegevens (zoals vingerafdrukken en gezichtsopnamen) van veroordeelde onderdanen van derde landen en staatlozen. Het is de bedoeling dat rechtshandhavingsinstanties via een online zoeksysteem gemakkelijk kunnen controleren of een persoon al dan niet in ECRIS TCN geregistreerd is. Het beheer van het systeem komt in handen van eu-LISA, een Europees agentschap dat verantwoordelijk is voor grootschalige informatiesystemen binnen het veiligheidsdomein. Het systeem is niet alleen bedoeld voor strafrechtelijke doeleinden, maar kan ook worden gebruikt voor bijvoorbeeld het uitvoeren van een antecedentenonderzoek.

https://bit.ly/2Kh3g91

Oprichting Common Identity Repository (CIR)
Op 16 april 2019 stemde het Europees Parlement in met de oprichting van een Common Identity Repository (CIR) voor biometrische gegevens van zowel EU-burgers als onderdanen uit derde landen. CIR moet het voor rechtshandhavingsinstanties eenvoudiger maken om elkaars database te raadplegen en deze met hun eigen database te vergelijken. De gegevens worden dus niet verplaatst naar één centrale database. Het CIR heeft betrekking op zowel verschillende bestaande als een aantal nieuw op te richten databases. Via het systeem zijn zowel identiteitsgegevens (zoals namen en geboortedatums) als biometrische gegevens (zoals vingerafdrukken en gezichtsopnamen) beschikbaar. Verschillende partijen, waaronder burgerrechtenorganisaties, hebben eerder felle kritiek geuit tegen de oprichting van het CIR.

https://bit.ly/2Xkt7AG

E-facturatie overheid
Sinds 18 april 2019 moeten overheidsinstanties en andere aanbestedende diensten (denk aan musea, onderwijsinstellingen, et cetera) elektronische facturen kunnen ontvangen en behandelen. De verplichting hiertoe vloeit voort uit de Europese Richtlijn elektronische facturering voor overheidsopdrachten (Richtlijn 2014/55/EU) die reeds in 2014 werd aangenomen. Vooralsnog waren lidstaten vrij om voor e-facturering eigen nationale voorschriften te stellen. Onder de nieuwe regels komt er echter een uniform wettelijk kader en ook een uniforme Europese standaard waaraan de e-facturen moeten voldoen. Op die manier wordt gewaarborgd dat er ook over landsgrenzen heen e-facturen ontvangen en verstuurd kunnen worden.

https://bit.ly/2QAlhQD

Tessa van Schijndel
Juridisch adviseur

Overheid | Cloud | Privacy

Wet op de medische hulpmiddelen is nog maar een jaar weg: wat moet er gebeuren?

Op 25 mei 2017 zijn de Verordeningen betreffende medische hulpmiddelen in werking getreden. Deze Verordeningen vervangen de Richtlijnen voor medische hulpmiddelen. De Verordening die specifiek ziet op medische hulpmiddelen voor in-vitrodiagnostiek wordt in dit artikel buiten beschouwing gelaten. Wel wordt ingegaan op de Verordening (EU) 745/2017 van het Europees Parlement en de Raad van 5 april 2018, hierna de Verordening. De verdere uitwerking van de Verordening wordt aan de lidstaten zelf overgelaten. In Nederland is daarom op 11 april 2019 een nieuw Wetsvoorstel medische hulpmiddelen aangenomen.[1] De wet treedt in werking op een later te bepalen tijdstip bij koninklijk besluit. Van de Verordening staat in ieder geval vast dat op 26 mei 2020 de overgangstermijn van drie jaar is verlopen. Vanaf dan dienen alle fabrikanten van medische hulpmiddelen zich aan de nieuwe regels te houden. We schreven er al eerder over, maar hoe zat het ook alweer?

Wat is een medisch hulpmiddel?
Medische hulpmiddelen zijn instrumenten, toestellen, apparaten en software die voor medische doeleinden worden gebruikt. Software wordt gezien als medisch hulpmiddel wanneer deze wordt gebruikt voor een diagnose, behandeling of indien deze een meetfunctie bevat.

Hoe zit het dan met apps? Medische apps kunnen medische hulpmiddelen zijn. Tegenwoordig bestaan er veel apps om je gezondheid of levensstijl te verbeteren. Het onderscheid tussen een medische app of een app met een algemeen doeleinde, zoals lifestyle- en welzijnsdoeleinde is niet altijd makkelijk te duiden. Hierdoor is het in veel situaties onduidelijk of een app gekwalificeerd moet worden als medisch hulpmiddel. In 2016 heeft de Europese Commissie een richtsnoer gepubliceerd om tekst en uitleg te geven met betrekking tot de oude Richtlijn. De Europese Commissie heeft aangegeven vernieuwde richtsnoeren te publiceren die uitleg geven aan de tekst van de nieuwe Verordening. Vooralsnog is er geen update gepubliceerd. Zo bleek bijvoorbeeld uit de uitleg in het richtsnoer uit 2016 dat apps die zich beperken tot opslag en archivering van data niet gekwalificeerd worden als medisch hulpmiddel, maar er zijn geen aanwijzingen te vinden dat dit onder de nieuwe Verordening nog steeds zo geldt. Ondanks dat de nodige tekst en uitleg nog niet beschikbaar is, is het wel belangrijk om al voor te sor-

1. In de laatste versie van de Richtlijn zijn bepaalde kleine bedrijven uitgesloten van haar verplichtingen, zie 'Kleine bedrijven worden gespaard'.

teren op de nieuwe regels. Fabrikanten moeten namelijk één jaar klinisch onderzoek verrichten en de app door een geschikte *notified body* laten beoordelen, voordat zij de app als medisch hulpmiddel op de markt kunnen brengen. Hieronder lichten we de belangrijkste aandachtspunten toe om te beoordelen of een app een medisch hulpmiddel is.

Een app is een medisch hulpmiddel indien de app door de fabrikant is bedacht om voor medische doeleinden te worden gebruikt.[2] Mede aan de hand van de *intended use* (het beoogde doeleinde) kan worden bepaald of de app een medisch hulpmiddel is en in welke klasse de app valt. Op basis hiervan zou een app die de hartslag monitort niet te kwalificeren zijn als medisch hulpmiddel als deze bedoeld is voor algemene fitnessdoelen van de gebruiker tijdens het hardlopen. Maar indien dezelfde app wordt gebruikt door artsen of fysiotherapeuten ter ondersteuning van hartrevalidatie, kan de app zich kwalificeren als medisch hulpmiddel indien de app dezelfde werking heeft en dezelfde risico's als een medisch hulpmiddel met zich meebrengt.[3] De *intended use* van de fabrikant geeft dus geen doorslag.

Ook wordt de definitie van een medisch hulpmiddel uitgebreid onder de nieuwe Verordening. Onder de medische doeleinden valt nu ook expliciet het voorspellen van een ziekte en het geven van een prognose. Bepaalde technologieën, bijvoorbeeld bij artificiële intelligentie, die in staat zijn en bedoeld zijn om het oplopen van een ziekte te voorspellen, kunnen nu binnen de definitie van een medisch hulpmiddel vallen.

In welke risicoklasse valt het medisch hulpmiddel?
Nadat de app wordt aangemerkt als een medisch hulpmiddel vindt er een risicoclassificatie van het hulpmiddel plaats. De Verordening kent vier risicoklassen: laag (klasse I), gemiddeld (klasse IIa en IIb) en hoog (klasse III).

Voor software heeft de Verordening voornamelijk gevolgen voor de risicoclassificatie van de apps. Software en dus ook apps, worden op basis van andere regels ingedeeld in risicoklassen. Veel apps zullen hierdoor in een hogere risicoklasse vallen. Daarvoor geldt dat een hardere toelatingsprocedure en een extra goedkeuring door een externe partij (*notified body*).

Nu de Europese Commissie nog geen vernieuwde richtsnoeren heeft gepubliceerd zijn er maar een beperkt aantal referentiekaders beschikbaar om te toetsen in welke klasse een app, die als medisch hulpmiddel gekwalificeerd wordt, terecht komt. Voor de toetsing is het afhankelijk van de specifieke omstandigheden van het geval of en in welke risicoklasse het medisch hulpmiddel geclassificeerd wordt. Factoren die van invloed zijn bij de classificatie van apps zijn het risico en het beoogde doel van de fabrikant.

Indien de app geen eigenschappen van individuele patiënten kan meten, valt de app in een lage risicoklasse. Een app die patiënten voorlicht over het voorkomen van sportblessures zal bijvoorbeeld in klasse I vallen. Deze medische hulpmiddelen vormen een laag risico. Hieronder vallen apps die geen beslisondersteuning voor diagnostische of therapeutische doeleinden bieden.

Een app die voorziet in beslisondersteuning bij een behandelplan van een patiënt, een app die fysiologische processen monitort of een app die een meetfunctie bevat zullen in klasse IIa vallen. Deze medische hulpmiddelen brengen een gemiddeld risico met zich mee.

Een app die op basis van een pijnscore zelf beslissingen neemt over een te volgen behandelplan voor patient zal in klasse IIb vallen. Deze apps hebben een hoger gemiddeld risico. Ook apps die voorzien in informatie die wordt gebruikt om beslissingen te nemen voor diagnostische of therapeutische doeleinde vallen in klasse IIb als deze beslissingen kunnen leiden tot een verslechtering van de gezondheid of een ingreep.

Een app die hoogstwaarschijnlijk in klasse III valt en een hoog risico met zich meebrengt is een app voorzien van artificiële intelligente beslisondersteuning in levensbedreigende situaties. Hieronder valt software welke informatie voor beslisondersteuning voor diagnostische of therapeutische doeleinden voorzien en daarbij kan leiden tot de dood of een verslechtering van de gezondheid.

Risicoklasse: welke eisen?
De eisen die voortvloeien uit de classificatie gelden voornamelijk voor de fabrikanten van de apps, die als medisch hulpmiddel gekwalificeerd worden. De fabrikant van de app is verantwoordelijk voor de kwaliteit en veiligheid ervan. Ook voor zorginstellingen en zorgverleners die intern hulpmiddelen ontwikkelen gelden

2. In de Richtlijn elektronische handel worden diensten die slechts informatie doorgeven ('*mere conduit*') onder bepaalde voorwaarden uitgesloten van aansprakelijkheid voor de inhoud van die informatie. Deze uitsluiting van aansprakelijkheid ging uit van de passieve rol van online platforms. De nieuwe Richtlijn legt platforms echter een actieve verplichting op.
3. Verordening (EU) 745/2017, overweging 12.

de eisen uit de Verordening, tenzij zij aan alle acht van de eisen voldoen uit artikel 5 lid 5 van de Verordening. Dit betekent onder andere dat de zorginstelling of zorgverlener het hulpmiddel niet mag overdragen aan een andere rechtspersoon en dat er een passend kwaliteitsmanagementsysteem wordt gebruikt. Indien aan deze twee en de andere zes voorwaarden wordt voldaan, gelden alleen de algemene veiligheids- en prestatie-eisen uit bijlage 1 van de Verordening.

Het toezicht op de naleving van de eisen ligt bij de Inspectie Gezondheidszorg en Jeugd. Enkele aandachtspunten waar fabrikanten rekening mee moeten houden zijn hieronder uitgewerkt:

CE-markering: een CE-markering is verplicht voor alle medische hulpmiddelen, ongeacht de risicoklasse waarin zij valt. Met deze markering wordt aangetoond dat het hulpmiddel voldoet aan de Europese eisen voor veiligheid, gezondheid, milieu- en consumentenbescherming. Als de app in een lage klasse valt, mag de fabrikant de app zelf certificeren middels een *self-assessment*. Dit betekent dat de fabrikant zelf verantwoordelijk is voor het testen en het controleren van de app of deze in overeenstemming is met de Verordening. Dit legt de fabrikant vast in de technische documentatie. Middels een EU-conformiteitsverklaring legt de fabrikant verantwoording af over de conformiteit van de app. Indien de app een meetfunctie bevat of in een hogere risicoklasse terecht komt, moet de app gecontroleerd worden door een *notified body*.

Klinische evaluatie en onderzoek: in het technisch dossier nemen de fabrikanten van de app een risicoanalyse op, maar ook dataverzamelingen en klinische evaluaties.

UDI-code en de EUDAMED: omdat ieder medisch hulpmiddel traceerbaar moet zijn, komt er een Europese databank: de EUDAMED. Ieder medisch hulpmiddel die onder de Verordening valt, krijgt een uniek identificatienummer, waarmee zij ingeschreven wordt in de EUDAMED.

Compliance officer: fabrikanten van medische hulpmiddelen moeten iemand aanstellen die verantwoordelijk is voor de naleving van de regelgeving. Aantoonbaar moet zijn dat deze persoon voldoende verstand van zaken heeft. De uitwerking van deze eis is nu nog niet bekend.

De bovenstaande eisen zijn niet volledig. Bij iedere app die zich kwalificeert als medisch hulpmiddel moet een afweging gemaakt worden welke eisen van toepassing zijn, afhankelijk van bijvoorbeeld het type medisch hulpmiddel, de organisatieomvang en de doelgroep die gebruik zal gaan maken van de app. Daarnaast moeten de algemene veiligheids- en prestatie-eisen niet vergeten worden. Zo is het bijvoorbeeld voor iedere hulpmiddel vereist dat de gebruiksaanwijzing moet zijn geschreven in een voor de beoogde gebruiker gemakkelijk te begrijpen taal. Al met al is er genoeg te doen en met nog maar een jaar te gaan, betekent dit dat fabrikanten, maar ook zorginstellingen en zorgverleners aan de slag moeten.

Ga dus na of uw hulpmiddel onder de Verordening valt, in welke risicoklasse deze valt en zorg dat aan de algemene veiligheids- en prestatie-eisen én aan de strengere eisen per risicoklasse worden voldaan. Om aan deze laatste categorie te voldoen moet onder andere een *notified body* worden gezocht en gestart worden met de klinische evaluatie en onderzoek.

Dit artikel is geschreven in samenwerking met stagiaire Elsbeth Penninkhof.

Linde Mensink
Juridisch adviseur

Privacy Marketing

Cookies plaatsen, toestemming vragen?

Cookies houden de gemoederen flink bezig. Adverteerders proberen op allerlei creatieve manieren hun conversie te behouden, terwijl de consument al die verschillende cookiebanners vaak als storend ervaart. Juristen hebben het druk met het formuleren van de correcte toestemmingsvraag en intussen schieten de nieuwe trackingtechnieken als paddenstoelen uit de grond. En toen verbood de Autoriteit Persoonsgegevens ook nog eens de *cookiewall!* Hoe voldoe je nu nog aan de cookiewetgeving zonder te veel conversie te verliezen?

Cookiewetgeving

Regelmatig verschijnen er artikelen in de media waaruit blijkt dat veel sectoren zich niet houden aan de cookiewetgeving. Maar wat houdt die cookiewetgeving nu precies in? Aan het gebruik van cookies zijn strenge (privacy)regels verbonden. De cookiewetgeving is vastgelegd in de Telecommunicatiewet (Tw)[1] en deels in de Algemene Verordening Gegevensbescherming (AVG), welke daarom bij velen bekend staan als 'de Cookiewet.'[2] Vanuit Europa wordt gewerkt aan nieuwe wetgeving: de ePrivacy Verordening (ePV). De ePV zal de cookiewetgeving uit de Tw te zijner tijd gaan vervangen en zal ervoor zorgen dat overal binnen de Europese Economische Ruimte (hierna: 'EER') dezelfde cookiewetgeving van toepassing zal zijn. Wanneer deze ePV uiteindelijk van toepassing zal zijn, is nog niet bekend. Voor meer informatie over de ePV, zie hiervoor: https://bit.ly/2EMpUT6.

Een cookie is een klein tekstbestand dat door een website op de harde schijf van je computer, telefoon of tablet wordt gezet op het moment dat je de site bezoekt. Dit klinkt simpel, maar dat is het niet. Er bestaat een veelheid aan technieken en het toepassingsbereik van de cookiewetgeving gaat dan ook verder dan enkel het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook pixels, Javascripts, Flash cookies, HTML5-local storage, web beacons, device fingerprinting en alle andere technieken waarbij gegevens worden geplaatst en/of uitgelezen. Slechts indien er in het geheel geen sprake is van het opslaan van gegevens dan wel het uitlezen van gegevens op de randapparatuur van de gebruiker is de Cookiewet niet van toepassing.[3]

Toestemming vragen

Voor de meeste organisaties is het inmiddels duidelijk dat ze toestemming moeten vragen voor het plaatsen van bepaalde (lees: de meeste) soorten cookies. Over hoe je die toestemmingsvraag nu moet inrichten bestaat nog veel onduidelijkheid. Toestemming is volgens de AVG pas rechtsgeldig wanneer deze aan de volgende voorwaarden voldoet:

- de toestemming moet specifiek zijn;
- de toestemming moet op informatie berusten;
- de toestemming moet in vrijheid gegeven zijn;
- de toestemming moet een actieve handeling zijn.

Pas op het moment dat de toestemming is gegeven (lees: er op een 'akkoord'-button is geklikt) mogen er cookies

1. Artikel 11.7a Telecommunicatiewet.
2. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).
3. Autoriteit Consument en Markt: veelgestelde vragen over de cookiebepaling: https://www.acm.nl/sites/default/files/old_publication/publicaties/14496_veelgestelde-vragen-cookiebepaling-november-2016.pdf.

worden geplaatst. Deze strenge voorwaarden worden in de praktijk meestal met een korreltje zout genomen. Wij zien verschillende inventieve constructies terugkomen, zoals: *"indien u verder klikt op onze website, gaat u akkoord met het gebruik van cookies die wij of derden plaatsen, waarmee wij of derden bepaalde persoonsgegevens verwerken voor doel A, B en C".*
Dit wordt ook wel impliciete toestemming genoemd en is niet (meer) toegestaan. Het toevoegen van in ieder geval een 'akkoord'- en een 'niet akkoord' (of: 'meer informatie')-button die de mogelijkheid biedt om te weigeren is vereist. Dit omdat het verder klikken op de website, hoewel ook dat een actieve handeling is, slechts impliciete toestemming inhoudt. Dat is dan ook niet voldoende.

Naast de impliciete toestemmingsvraag, zien we met enige regelmaat dat toestemming wordt afgedwongen via de zogeheten 'cookiewall.' Ondanks het verbod op de cookiewall dat de Autoriteit Persoonsgegevens[4] op die beruchte donderdagmiddag in mei '19 uitsprak, wordt deze beeldvullende pop-up nog steeds door een aantal grote partijen gebruikt. Een cookiewall maakt toegang tot websites onmogelijk totdat de websitebezoeker de beeldvullende 'wall' weg klikt door toestemming te geven voor trackingcookies. De reden van deze uitspraak van de AP: het voldoet niet aan de AVG. Het geven van toestemming is dan namelijk niet langer te beschouwen als 'vrij.'

Waar de focus tegenwoordig vooral ligt op het vragen van toestemming via de cookiebanner, is het informeren via de (privacy- en) cookieverklaring minstens zo belangrijk. De AVG[5] geeft een aantal minimale vereisten voor de cookieverklaring. Ook de toezichthouders op dit gebied, de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt, hebben zich daarover uitgelaten. In een cookieverklaring moeten in ieder geval de volgende punten terugkomen:
- de doeleinden voor het gebruik van de cookies;
- de grondslag voor het plaatsen van de cookies (toestemming);
- de soorten persoonsgegevens die via de cookies worden verzameld en verwerkt;
- de ontvangers van de gegevens (juridische entiteiten);
- de passende waarborgen voor verwerkingen buiten de EER, en hoe deze kunnen worden geraadpleegd;

4. Autoriteit Persoonsgegevens: websites moeten toegankelijk blijven bij weigeren tracking cookies, nieuwsbericht 07 maart 2019: (https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#-mag-ik-als-organisatie-een-cookiewall-gebruiken-7111)
5. Artikel 13 AVG.

- de bewaartermijnen;
- de rechten van betrokkenen (en de wijze waarop betrokkenen deze kunnen uitoefenen);
- zo veel nadere informatie als nodig is om websitebezoekers een eerlijk beeld te geven van de gegevensverwerking.

Cookiecare
Gericht adverteren is inmiddels de wereldwijde standaard voor online advertising. Geen wonder dat organisaties zo opkijken tegen de Cookiewet: cookies zijn namelijk een grote bron van inkomen. Vooral wanneer jouw businessmodel grotendeels bestaat uit het personaliseren van advertenties via cookies en jouw bestaande constructie opeens verboden is, is de paniek wel voor te stellen.

De meningen onder de (niet-)juristen zijn dan ook enorm verdeeld. Waar de een vindt dat er niets mis is met een cookiewall omdat dit een manier is om te 'betalen met data' voor de content van de 'gratis' website, benadrukt de ander weer hoe vergaand de inbreuk op de privacy bij gebruik van tracking en personalisatie kan zijn. Daarnaast speelt de vraag of je als consument eigenlijk überhaupt wel kunt weten waar je nu precies toestemming voor geeft. Hoe uitgebreid een banner ook is, het blijft lastig voor consumenten om een voorstelling te maken van de precieze werking van tracking en hoe ver dit kan gaan.

Het belangrijkste is dat je als organisatie transparant bent. Wij zijn ervan overtuigd dat dit mogelijk is zonder al je conversie te verliezen. ICTRecht heeft hiertoe een nieuwe dienst opgezet: *Cookiecare*. Voor alle bedrijven en webwinkels die gebruikmaken van cookies is het belangrijk om de privacyverklaring up-to-date te houden en een duidelijke cookieverklaring te formuleren bij soms complexe regels rondom analytische en tracking tools. Wij hebben voor een groot aantal organisaties een cookie-inventarisatie mogen uitvoeren. Naar aanleiding daarvan hebben wij de bedrijven kunnen helpen aan een rechtsgeldige toestemmingsvraag voor de cookiebanner en een cookieverklaring die voldoet aan alle vereisten.

ICTRECHT
adviesbureau

Benieuwd of uw webshop of website voldoet aan de vereisten voor het vragen van rechtsgeldige toestemming voor, en het verdere gebruik van cookies? ICTRecht biedt de dienst ‘Cookiecare’ aan!

De dienst ‘Cookiecare’ bestaat uit:

- Inventarisatie van de geplaatste cookies
- Advies over de implementatie van de voorgestelde aanpassingen in uw webwinkel of website
- Opstellen van een cookieverklaring dan wel aanpassen van de privacyverklaring

Meer weten over deze dienst?

Meer informatie is te vinden op: ictrecht.nl/cookiecare.
Of neem contact op met één van onze privacy experts via 020 663 1941 of info@ictrecht.nl.

Samantha van de Stouwe
Juridisch adviseur

Contracteren | Innovatie

Smart contracts: hoe werkt het en wat kunt u ermee?

De term smart contract wordt vaak samen genoemd met de term blockchain, in ieder geval in de juristenwereld, maar wat velen niet weten is dat smart contracts al ver voor de opkomst van de blockchaintechnologie zijn geïntroduceerd. Om precies te zijn in 1994 door Nick Zsabo.

Een voorbeeld van het gebruik van smart contract is in de handel van cryptocurrencies. De balans staat in een smart contract en zodra er een bepaalde input komt (er wordt voldaan aan de voorwaarden van betaling) wordt een bedrag overgemaakt naar een andere wallet. Andere mogelijkheden zijn contracten zoals een auteursrecht overdrachtsakte die op de blockchain opgenomen kunnen worden. Maar hoe werkt zo'n smart contract eigenlijk?

Kenmerken

Nick Zsabo omschreef de smart contract als volgt: *"A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.[1]"*

Een smart contract is niet meer dan programmeercode die is opgenomen in een blockchain en hier wordt uitgevoerd. In een smart contract zijn rechten/verplichtingen opgenomen die aan voorwaarden gekoppeld worden. Zodra deze voorwaarden (zoals een termijn die is verstreken) vervuld worden, zullen de rechten/verplichtingen automatisch door het smart contract worden uitgevoerd. Een smart contract zal dus altijd dezelfde output geven bij een bepaalde input en beginwaarden. Smart contracts zijn opgenomen op blockchains en hiermee transparant. Je kunt als partij de code van het contract altijd controleren. Bovendien biedt een smart contract zekerheid. De smart contract wordt altijd uitgevoerd bij een bepaalde input. De blockchain met haar nodes zorgt ervoor dat de uitkomst voortdurend wordt bevestigd. Bij papieren contracten kunnen partijen wat hen volgens het contract is opgedragen nalaten. Dit is niet mogelijk bij een smart contract, wat hiermee een groot voordeel is.

Juridische status

Om te bepalen wat de juridische status van een smart contract is, dienen we eerst te kijken naar de eisen voor de totstandkoming van een overeenkomst.
Een overeenkomst komt tot stand door aanbod en aanvaarding waarbij de wilsovereenstemming tussen partijen van belang is.[2] Uiteraard dient de overeenkomst ook voldoende bepaalbaar te zijn.[3] Een overeenkomst kan

1. N. Szabo, 'Formalizing and Securing Relationships on Public Networks', 1 september 1997.
2. Art. 3:33 BW jo. 6:217 BW.
3. Artikel 6:228 BW.

mondeling zijn, maar kan ook schriftelijk geschieden door middel van een contract. Dit laatste is verstandiger met betrekking tot de bewijsvoering. Eén van de functies van een contract is de directe uitvoering van een overeenkomst. Bijvoorbeeld de overdracht van een auteursrecht dat dient te geschieden bij akte. Schrijf je het op, dan is het auteursrecht direct overgedragen. Hierbij is het verschil tussen een papieren contract en een smart contract dus minimaal omdat het 'papieren' contract net zoals een smart contract, de uitvoering betreft.

Het bepaaldheidsvereiste zal bij een smart contract niet snel tot problemen leiden. Het feit dat het geschreven is in programmeercode leidt niet tot een ander oordeel. Of het nu in programmeercode is geschreven of in het Noors, het is gewoon een contract in de taal van de programmeercode. En in deze programmeercode staan rechten/verplichtingen en voorwaarden omschreven. De wilsovereenstemming bij smart contracts zal wel sneller tot problemen leiden doordat de taal programmeercode is. Het is zeer goed mogelijk dat partijen of een van de bij het smart contract betrokken partijen geen of onvoldoende kennis heeft van de programmeertaal. Hierdoor is het goed mogelijk dat de wil niet overeenstemt met wat uiteindelijk is opgenomen in de code met het gevolg dat er bijvoorbeeld een beroep gedaan wordt op dwaling.[4]

4. Artikel 6:228 BW.

In een gemiddeld contract komen bepalingen over de uitvoering, verplichtingen, verboden, bevoegdheden en ordeningsbepalingen voor. Bepalingen over de uitvoering van een contract, verplichtingen en verboden zijn over het algemeen goed in te regelen in een smart contract. Je kunt bijvoorbeeld opnemen onder welke omstandigheden een persoon verplicht is om een bedrag te bepalen of wanneer iets niet mag. Bij de uitvoering doet het smart contract het ook direct zelf. De bevoegdheidsbepalingen en ordeningsbepalingen geven echter wel problemen. Terwijl de bevoegdheidsbepalingen aangeven dat iets mag maar niet hoeft, geven ordeningsbepalingen context aan een dergelijk contract. Denk hierbij aan de rechts- en forumkeuze. Vooral deze bepalingen zijn moeilijk in te regelen in een smart contract.

Een ander nadeel is dat de code van een smart contract onveranderlijk is zodra het is opgenomen op de blockchain. Alle mogelijke onverwachte gebeurtenissen zullen dus vooraf al opgenomen moeten worden om de automatische uitvoering van ongewenste uitkomsten te voorkomen. Dit is vooral lastig bij de complexere overeenkomsten. Een smart contract leent zich daardoor vrijwel alleen voor binaire termen. Voorbeelden van niet binaire termen zijn onder meer een inspanningsverplichting, de redelijkheid en billijkheid en de beginselen van behoorlijk bestuur. Er zou dan alsnog uitgeschreven moeten worden wat hiermee

bedoeld wordt en wanneer er sprake van is terwijl dit heel lastig is. Het opnemen van dergelijke termen (of juist het weglaten hiervan) kan dus leiden tot voor de betrokken partijen ongewenste uitkomsten.

De onveranderlijkheid van een smart contract vergroot de kans op problemen in de uitvoering. Een smart contract kan gewoon niet gestopt worden. Stel je wilt allebei van het contract af. In een 'papieren' contract ben je niet verplicht om een dergelijke bepaling op te nemen omdat je samen instemt om te stoppen. Heb je dit echter niet ingebouwd in een smart contract, dan loopt het contract gewoon door. Het is niet te stoppen, ook al wil je dat wel. Hetzelfde geldt voor een ontbindingsverklaring. Hoewel na een dergelijke verklaring een smart contract er juridisch niet meer is, loopt deze in de praktijk wel gewoon door. Dit geldt ook voor vernietigingshandelingen. Dat je een uitspraak van een rechter niet ten uitvoer kan leggen doet niks af aan deze uitspraak. We lopen hier dus eigenlijk niet tegen juridische problemen aan, maar vooral tegen praktische problemen.

Mogelijke oplossingen voor bovengenoemde problemen zijn het opnemen van alle situaties die zich zouden kunnen voordoen of de smart contracts te beperken tot enkel de binaire bepalingen. Een normaal contract wordt dan gebruikt voor de niet-binaire bepalingen en hierin wordt verwezen naar het smart contract dat de binaire bepalingen uitvoert. Een andere mogelijkheid is gebruikmaking van oracles. Oracles leveren input van buitenaf aan een smart contract. Het is een externe informatiebron en kan zowel een technische bron zijn zoals een database als een persoon zoals een (ICT-)jurist, rechter of (IT)-notaris. Partijen bij het smart contract vertrouwen op de waarheidsvinding van het oracle nu deze de juiste informatie dient aan te leveren. In het smart contract kan bijvoorbeeld ook een interface gebouwd worden naar een oracle voor geschilbeslechting. Bijvoorbeeld de rechter die dan een bindende uitspraak kan doen. Het smart contract krijgt vervolgens een ondertekende instructie in programmeertaal vanuit het oracle wat er gedaan dient te worden.

Aansprakelijkheid

Dat het flink mis kan gaan bij smart contracts is wel gebleken uit de DAO-affaire uit 2016. Een DAO (Decentralized Autonomous Organization) codificeert het beslissingsproces, regels en voorwaarden van een organisatie zodat de noodzaak tot het hebben van een bestuur of managementteam wegvalt. De leiding verloopt dan op basis van de vastgelegde voorwaarden in de smart contracts. Opdrachten en afspraken worden door de smart contracts gedecentraliseerd opgeslagen en uitgevoerd. Heeft een DAO succes en heb je hierin geïnvesteerd (met bijvoorbeeld ethers) dan krijg je een winstpercentage.

Een persoon had een fout ontdekt in de programmeercode van een van de smart contracts van een DAO en heeft hierdoor miljoenen dollars aan Ether naar zichzelf kunnen doorsluizen. Deze gebeurtenis heeft flink wat stof doen opwaaien. Hoewel de onveranderlijkheid een van de kerneigenschappen van de blockchain is en daardoor zekerheid biedt is er gekozen voor een hard fork. Dit betekent een splitsing in de blockchain met een nieuwe en een oude blockchain. Het geld dat weggesluisd was is in de nieuwe blockchain via een nieuw smart contract teruggehaald waardoor investeerders hun Ether terug konden krijgen.

Fouten in smart contracts zijn dus een van mogelijkheden tot aansprakelijkheidsstelling. Je bent aansprakelijk bij het plegen van een onrechtmatige daad of wanneer een wanprestatie kan worden toegerekend. Het is dus van belang om in een overeenkomst met de programmeur van het smart contract de aansprakelijkheid voor programmeerfouten op te nemen. Hiernaast kunnen er ook programmeerfouten optreden in de blockchain zelf of kunnen blockchains gehackt worden. Als maker van een dergelijke blockchain is het daarom verstandig om aansprakelijkheidsuitsluitingen voor dergelijke situaties in de algemene voorwaarden op te nemen. Hierbij is het wel van belang dat de identiteit van de wederpartij met voldoende zekerheid is vast te stellen.

Conclusie

Er wordt wel gezegd dat smart contracts de huidige contracten zullen vervangen en juristen overbodig zullen maken. Ik denk echter dat het zo'n vaart niet loopt. Hoewel smart contracts zorgen voor meer transparantie en zekerheid tussen partijen zijn er ook valkuilen. De smart contracts kunnen programmeerfouten bevatten of partijen zijn bepalingen vergeten met alle gevolgen van dien. Hoe dan ook blijven juristen en rechters hier om de hoek kijken en dan heb ik het nog niet eens over de eigenlijke onmisbare oracles in de vorm van een (IT-)notaris, (ICT-)jurist of rechter. Smart contracts kunnen zeker handig zijn, maar zijn zeker niet zo "smart" dat bijvoorbeeld juristen of notarissen erdoor vervangen kunnen worden. Wel is het zeker een interessante ontwikkeling die we moeten omarmen en door ontwikkelen.

Tim Wokke
Juridisch adviseur

E-commerce Overheid

Belangrijke aandachtspunten bij cross-border e-commerce

Sinds 2015 is het stimuleren van cross-border e-commerce een van de belangrijkste prioriteiten binnen de Europese Unie. Het maakt een onderdeel uit van de strategie tot het creëren van één grote Europese markt, de “Digital Single Market”. Om dit te bereiken zijn inmiddels tientallen verordeningen en richtlijnen aangenomen om bestaande cross-border belemmeringen weg te nemen. Voor e-commerce partijen die tot nu toe huiverig waren om over de grens te verkopen, is het nu dan ook een goed moment de mogelijkheden daartoe te gaan inventariseren en in kaart te brengen met welke regels zij te maken hebben. In dit artikel worden enkele belangrijke (juridische) aandachtspunten besproken.

Algemeen
Bij het bepalen van welke regels relevant zijn zal een verkoper allereerst vast moeten stellen wat er geleverd wordt, aan wie en waar. Gaat het om verkoop van fysieke producten of levering van (digitale) diensten? Is de afnemer een consument of zakelijke partij? En voor welke landen geldt het aanbod? Afhankelijk van het antwoord zullen bepaalde regels (en uitzonderingen) namelijk wel of niet relevant zijn.

Aandachtspunten
Toepasselijke recht en bevoegde rechter
Allereerst zal een verkoper in zijn algemene voorwaarden moeten bepalen welk recht van toepassing is en welke rechter bevoegd is bij eventuele geschillen. Keuze voor een eigen rechter heeft overigens niet altijd effect, want een consument blijft altijd de mogelijkheid behouden om een geschil in zijn woonplaats aanhangig te maken. Daarnaast zal keuze voor het eigen rechtstelsel bij B2C-transacties geen afbreuk kunnen doen aan eventuele dwingende nationale regels die de consument meer beschermen. Denk bijvoorbeeld aan de Nederlandse wettelijke garantieregeling die over het algemeen gunstiger is dan de Duitse regeling.

De rechts- en forumkeuze zijn voornamelijk van belang voor B2B-transacties. In dat kader is het ook nog van belang te bepalen of het Weens Koopverdrag - dat automatisch van toepassing is op internationale verkoopovereenkomsten - buiten werking wordt gesteld. Over het algemeen wordt dit verdrag wel als ‘gunstig’ voor verkopers beschouwd.

Taal van het contract
Verkopers kunnen richting zakelijke afnemers zelf bepalen in welke taal zij wensen te contracteren. Het belangrijkste is dat de inhoud van de overeenkomst (en eventuele algemene voorwaarden) voor beide partijen begrijpelijk is. Een combinatie van talen, zoals een Duitstalig aanbod en Spaanstalige algemene voorwaarden, wordt dan ook afgeraden.

Ten aanzien van consumenten is per lidstaat bepaald in welke taal er mag worden gecontracteerd. Zo moet een webshop die zich richt op de Franse, Portugese of Spaanse markt, alle contractuele informatie (het aanbod en algemene voorwaarden) in die taal aanbieden - waar dat in Italië alleen op verzoek van de consument hoeft.

Geoblocking

Bij het inrichten van een webshop moet rekening gehouden worden met de nieuwe geoblocking regelgeving. Sinds december 2018 is het namelijk niet meer toegestaan om buitenlandse bezoekers te weigeren of zonder toestemming automatisch door te geleiden naar een variant in diens eigen taal. Iedere internationale bezoeker, consument of zakelijk, moet de mogelijkheid hebben aankopen te doen tegen dezelfde betaal- en leveringsvoorwaarden die gelden voor gelijkwaardige nationale bezoekers. Een Fransman die bij een webshop wil bestellen die uitsluitend in de Benelux levert, moet dit kunnen doen. De webshop is echter niet verplicht bezorging naar Frankrijk te faciliteren. Als de webshop uitsluitend iDEAL accepteert, is het aan de Fransman om daar beschikking over te krijgen. Voldoende is dat de webshop de Fransman dezelfde voorwaarden biedt. Het is dan ook nog steeds toegestaan om landspecifieke webshops te exploiteren, met afwijkende prijzen per land.

In enkele gevallen is geoblocking nog wel geoorloofd, bijvoorbeeld om te voorkomen dat het aanbod beschikbaar komt in landen waar het betreffende product of dienst verboden is. Denk bijvoorbeeld aan het Griekse verbod op de e-sigaret of (vooralsnog) het aanbieden van online kansspelen in Nederland.

Betaaltoeslagen

Het rekenen van betaaltoeslagen is niet altijd toegestaan. Dit is afhankelijk van het gekozen betaalinstrument of betaaldienst en het type gebruiker (consument of zakelijk). Enige zekerheid is dat consumenten in heel Europa in ieder geval niet meer extra belast mogen worden voor het gebruik van VISA-, Mastercard- en simpele SEPA-transacties. Het is echter zo dat elke lidstaat de mogelijkheid heeft om dit verbod breder te trekken. Zo lijkt het verbod in België vooralsnog op álle betaalmiddelen betrekking te hebben, en wordt er in Duitsland momenteel geprocedeerd over de vraag of PayPal hieronder valt. Webshops die over de grens gaan leveren en betaaltoeslagen wensen te rekenen, zullen dit dan ook per land moeten inventariseren. Om hierbij van dienst te zijn, bieden sommige payment service providers tooling aan die 'live' controleert of een toeslag mag worden gerekend.

Belastingregels

Bij verkoop binnen Nederland is een ondernemer gebonden aan de Nederlandse btw-verplichtingen. Bij internationale verkoop rijst de vraag welke belastingregels van toepassing zijn, welk tarief gerekend moet worden en in welk land btw moet worden afgedragen.

Voor zakelijke leveringen is dit relatief eenvoudig te bepalen. Het uitgangspunt is namelijk dat deze levering in Nederland belast is met 0% btw. De btw-verplichting wordt in wezen verlegd naar de koper in de andere lidstaat. Deze moet btw-aangifte en afdracht doen tegen het in dat land geldende percentage.

Voor levering aan consumenten in een andere lidstaat ligt het wat complexer. In beginsel moet de verkoper gewoon de Nederlandse btw in rekening brengen en afdragen. Dit wordt slechts anders als omzet naar een bepaald land boven een specifiek drempelbedrag uitkomt (deze drempelbedragen verschillen per land). Vanaf dat moment moet de verkoper het btw-tarief van het EU-land in rekening brengen en daar afdragen. Dit betekent dat de verkoper zich ook in dat land moet registreren bij de lokale belastingdienst.

Deze administratieve lasten zijn in 2015 al deels verlicht. Aanbieders van digitale diensten (bijvoorbeeld *streaming*) hoeven uitsluitend aangifte en afdracht te doen in eigen land. Wel moet de verkoper nog steeds het belastingtarief rekenen dat geldt in het land waar de koper is gevestigd (zodra het drempelbedrag is bereikt). De lokale belastingdienst verdeelt de opbrengsten vervolgens over de verschillende landen waar is geleverd. Om ook de overige e-commerce sector van dienst te zijn, wordt deze vereenvoudiging per 2021 uitgebreid tot de verkoop van alle diensten en producten. Vanaf dat moment hoeft een verkoper zich dus niet meer in een ander EU-land te registreren.

Retourzendingen
Bij B2C-transacties spelen retourzendingen en de kosten die daarmee gepaard gaan een steeds grotere rol. Mocht een consument gebruikmaken van zijn wettelijke herroepingsrecht, dan hoeft hij de kosten van het terugsturen alleen te dragen indien de verkoper dit vooraf duidelijk had vermeld. Bij internationale levering is het dan ook van belang op informatieve pagina's volledige informatie te verschaffen over het herroepingsrecht en deze randvoorwaarden.

Retourzending speelt ook een rol bij garantieclaims. Wanneer een product niet voldoet aan de redelijke verwachtingen van de consument, dan kan de consument de verkoper aanspreken voor vervanging of reparatie, of in het uiterste geval teruggave van het aankoopbedrag. Alle daarmee gepaarde kosten komen voor rekening van de verkoper.

Tot slot
De Europese markt is de afgelopen jaren voor de e-commerce sector een stuk aantrekkelijker gemaakt. Desondanks blijven er veel verschillen bestaan tussen de nationale regelgeving, wat het lastig maakt de Europese markt te betreden. Omdat deze drempel vooralsnog niet weggenomen is, blijft het dan ook nog steeds van belang te oriënteren welke markt het meest geschikt is en waar de minste (juridische) obstakels zijn.

“De opleiding beslaat een grote hoeveelheid en goede mix aan onderwerpen en vaardigheden waar je als FG mee te maken hebt. Daarbij wordt ook de diepte ingegaan, waardoor je leert een kwestie zelfstandig te beoordelen. Ik heb vol vertrouwen in de kennis die ik tijdens de opleiding heb opgedaan.”

Bob van Knippenbergh
Functionaris Gegevensbescherming
bij Zermelo Roostermakers

15 jaar ICTRecht vieren wij met extra scherpe prijzen!

Specialiseer u tot FG/DPO

De ICTRecht Academy biedt u een opleiding tot Functionaris Gegevensbescherming (FG) – ook wel bekend als Data Protection Officer (DPO). In 12 trainingsdagen, verspreid over drie maanden (start september 2019), doet u gespecialiseerde kennis op over de Europese privacywetgeving (AVG/GDPR) en de vertaling van deze wet naar de dagelijkse praktijk. Wij stomen u klaar voor de positie als FG/DPO.

Kijk voor meer informatie op: ictrecht.nl/opleiding-fg-dpo

ICTRECHT
academy

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Internetrechtspraak

Rechtbank Midden-Nederland 13 september 2013
(NAW-gegevens oplichter)
Gepubliceerd 11 maart 2019, een persoon stelt te zijn opgelicht door een Marktplaatsverkoper, en eist van de SNS bank – die het bankrekeningnummer bij de advertentie beheert – de NAW-gegevens van de oplichter zodat hij deze een proces kan aandoen. De rechtbank beoordeelt de aanvraag onder de Wbp (artikel 8 sub f, identiek aan artikel 6 lid 1 sub f AVG) en laat de belangenafweging in het nadeel van eiser uitvallen. Cliënten moeten kunnen vertrouwen op hun banken en dit vertrouwen dient onder meer in te houden dat hun persoonsgegevens slechts in zeer uitzonderlijke situaties aan derden mogen worden verstrekt. In dat kader heeft eiser onvoldoende aangetoond dat in dit geval sprake is van een zeer uitzonderlijke situatie. Tussen de regels door volgt de rechtbank ook het Lycos/Pessers kader, waarmee tot dezelfde conclusie gekomen wordt.

https://bit.ly/2ZwazxX

Rechtbank Rotterdam 21 februari 2019
(Review op Facebook)
Een bedrijf verhuurt beveiligingssystemen aan het MKB, onder meer aan een partij die daar ontevreden over is. Zij plaatst op Facebook een recensie met onder meer *"Dit bedrijf geeft geen veilig gevoel ze laten je inloggen met je e-mail adres en wachtwoord van jou e-mail. Iedereen kan zo je mail in wat bij mij gebeurd is. Ik ben gehackt en al me persoonlijke informatie ligt op straat".* Het bedrijf maakt bezwaar omdat zij de klant niet gehackt heeft. De rechtbank leest het bericht anders: zij is gehackt door iemand, en wel nadat dit bedrijf haar diensten heeft verleend. Zij mag dan ook ontevreden zijn met de beveiligingsdienstverlening. Ook de verklaring dat "opzeggen bijna onmogelijk is", is niet zonder meer onrechtmatig. Uit de context, in het bijzonder de verklaring dat vooruit was betaald en dat de ondernemer het reeds vooruit betaalde bedrag niet zou terugkrijgen, blijkt voldoende dat deze bewering betrekking heeft op een reeds overeengekomen en al betaalde periode.

https://bit.ly/2FfNcRB

Rechtbank Rotterdam 22 februari 2019
(OvJ inzage in Telegram-berichten)
Gepubliceerd 9 april 2019, in een strafzaak wil de officier van Justitie toegang tot berichten in een Telegram-account. Vanwege end-to-end encryptie kan hij deze niet bij de provider (Telegram) vorderen, daarom wil de officier toegang tot het account van de verdachte. De rechtbank neemt in overweging de omstandigheid dat op grond van op handen zijnde wetgeving in een digitale omgeving met machtiging van de rechter-commissaris verderstrekkende opsporingsbevoegdheden mogelijk zullen worden, en geeft daarom toestemming., met dien verstande dat de machtiging uitsluitend betrekking heeft op de gegevens die op de dag van de aanvraag bij de rechter-commissaris beschikbaar waren.

https://bit.ly/2KlteZS

Rechtbank Limburg 6 maart 2019
(Onrechtmatige beelden als bewijs)
Een werkgever installeert een verborgen camera vanwge een verdenking van verduistering van goud en andere waardevolle metalen die het bedrijf uit afval wint. Hij volgt daarbij niet de wettelijke regels en vraagt de OR niet om instemming. Een werknemer die wordt ontslagen, maakt bezwaar tegen gebruik als bewijs van die onrechtmatige beelden. Desondanks laat de rechtbank de beelden toe als bewijs. Het zonder toestemming maken van video-opnamen van een persoon is weliswaar op zichzelf aan te merken als onrechtmatig, maar het belang van de waarheidsvinding prevaleert in dit geval. De verdenking is een ernstige (ontvreemding van bedrijfseigendommen), het bedrijfsbelang voor het bedrijf bij het vinden van de dader(s) is ontegenzeggelijk groot, en de werknemer is slechts op één specifieke plek met één specifiek doel gefilmd en niet langer dan noodzakelijk, zodat aan het proportionaliteitsvereiste is voldaan. Daar komt bij dat een paar maanden eerder het personeel uitdrukkelijk is gewaarschuwd tegen het ontvreemden van bedrijfsspullen, waarbij het gevolg van overtreding van dit verbod in het vooruitzicht is gesteld.

https://bit.ly/2FeAXoT

Rechtbank Rotterdam 7 maart 2019
(Eigendom Facebookpagina en -groep)
De politieke partij ONS.Vlaardingen kwam in conflict met het uit de fractie gezette raadslid Tim Thiel: die weigerde de beheerrechten van de ONS-Facebookpagina en een bijbehorende discussiegroep af te staan. Hij zag deze als zijn persoonlijke investering en succes. Juridisch gezien is onduidelijk hoe een dergelijke pagina of groep überhaupt te kwalificeren – zaak, vermogensrecht, overeenkomst van opdracht, licentie onder auteursrechten – maar de rechtbank pakt het pragmatisch aan. Degene die een pagina aanmaakt is in beginsel de beheerder ("eigenaar") van die pagina, tenzij er concrete opdrachten zijn gegeven of je bindend hebt toegezegd deze over te dragen. De officiële partijpagina is derhalve van de partij zelf, deze is in 2014 gemaakt nog voordat Thiel lid werd, en hij kreeg de vraag om deze te gaan beheren. Maar de groep is door hem zelf aangemaakt en beheerd, en doet zich niet voor als officieel. Deze mag hij behouden.

https://bit.ly/2WMfjxR

Rechtbank Den Haag 7 maart 2019
(Card sharing Ziggo)
De verdachte heeft gedurende een periode van ongeveer vijf jaar en acht maanden illegaal tegen betaling Ziggo kanalen aangeboden aan tussen de 342 en 562 andere gebruikers door card sharing. De verdachte heeft de card sharing mogelijk gemaakt door zijn legale Ziggo-abonnement via een zogenaamde Dreambox te ontsleutelen.

https://bit.ly/2XQD4WR

Rechtbank Den Haag 7 maart 2019
(DDoS aanval als afpersing)
De verdachte heeft met een botnet DDoS-aanvallen op verschillende websites uitgevoerd, en daarbij van de beheerders bitcoin verlangd om de aanvallen te laten stoppen. De rechtbank merkt dit botnet aan als een technisch hulpmiddel in de zin van de voorbereidingshandelingen van artikel 139d Strafrecht. Hoewel de wettekst spreekt over een technisch hulpmiddel, is de rechtbank gelet op de wetsgeschiedenis en het doel van het Cybercrimeverdrag van oordeel dat beoogd is ook een botnet, zoals het Mirai botnet dat de verdachte voorhanden had, onder de strafbaarstelling van deze artikelen te brengen.
De rechtbank is voorts van oordeel dat een DDoS-aanval een vorm van cybercriminaliteit is die zonder meer kan worden gekwalificeerd als geweld in de zin van artikel 317 van het Wetboek van Strafrecht.

https://bit.ly/2Im4w9C

Rechtbank Amsterdam 28 maart 2019
(Dreiging met school shooting)
Op 11 december 2018 is informatie ontvangen van de FBI uit de Verenigde Staten van Amerika dat op 5 december 2018 om 18.06 uur (lokale tijd) een verontrustend bericht over een mogelijke school shooting is geplaatst op een YouTube groepspagina. Het bericht luidt: *"Fuck you man just when I was planning my school shooting you come out with motivational bs (this is actually no joke)".* Via een gekoppeld Google-account weet de politie een verdachte te achterhalen. De rechtbank acht de inhoud van de tekst op zichzelf zeer bedreigend. Verdachte schrijft dat hij een school shooting aan het plannen is/was. Eerder hebben school shootings plaatsgevonden, bijvoorbeeld in Amerika en Duitsland, nadat die eerst waren aangekondigd op internet. Deze omstandigheid in combinatie met de tekst maakt dat bij iedere lezer van dit bericht de redelijke vrees kon ontstaan dat er daadwerkelijk een school shooting zou plaatsvinden. De tekst heeft de opsporingsdiensten gealarmeerd en tot nader onderzoek geleid en dat onderstreept de dreigende aard van het bericht. In beginsel kan elke school, iedere leerling en elke docent zich door dit bericht aangesproken voelen. Bij de stukken bevindt zich echter geen bewijsmiddel waaruit volgt dat iemand uit deze groep het bericht heeft gezien. Onder deze omstandigheden komt de rechtbank tot het oordeel dat sprake is van een strafbare poging.

https://bit.ly/2MQ6H9r

Rechtbank Midden-Nederland 4 april 2019
(Wat is onderhoud aan software)
Het bedrijf Rainbow biedt onderhoud aan op software van derden, waaronder een inmiddels failliet gegaan bedrijf. De auteursrechten op de software worden door een ander overgenomen, die vervolgens Rainbow

aanspreekt op inbreuk: het onderhouden van de software zonder bij haar afgenomen licentie. De rechtbank ziet in artikel 45j Auteurswet een goede grond voor Rainbow en haar klanten: een rechtmatige verkrijger mag de software gebruiken en onderhouden voor foutherstel indien “noodzakelijk voor het beoogde doel”. Onduidelijk uit de stuken is wat het beoogde doel was (dit is een bekend en lang bestaand probleem, al vaak gesignaleerd in de literatuur). De rechtbank wijst tussenvonnis en laat partijen gelegenheid zich hierover uit te laten.

https://bit.ly/2MSbaZs

Hoge Raad 9 april 2019
(Computervredebreuk door XSS?)
Een bedrijf constateert op zeker moment dat zij wordt aangevallen via internet, middels een automatische scan van een web vulnerability scanner genaamd Acunetix. Later blijkt ook dat er middels cross site scripting en directory traversal aanvallen op de website zijn uitgevoerd. De Hoge Raad vindt dit te weinig om van computervredebreuk te spreken: de enkele omstandigheid dat de verdachte met behulp van een scan-programma de website van de aangever op kwetsbaarheden heeft onderzocht, waarvan een aantal werd geblokkeerd en dat als gevolg daarvan 'niet ondenkbaar is dat er een geslaagde aanval heeft plaatsgevonden' volstaat niet als overtuigend bewijs van binnendringen.

https://bit.ly/2RkUXKS

Rechtbank Midden-Nederland 10 april 2019
(Foto-inbreuk)
Een persoon plaatst een foto op zijn website en krijgt een sommatie met schadeclaim van Permission Machine bvba voor een slordige 800 euro. Dat er sprake is van inbreuk staat vast, de hoogte van de vergoeding wordt betwist. De rechtbank hanteert hiervoor de tarievenlijst van stichting Foto Anoniem (omdat dit niet wordt betwist) en neemt de prijs voor het kleinste formaat (€185) met daarop een korting van 25%, zodat de schadevergoeding 173 euro wordt. Verder past de rechtbank het liquidatietarief toe gezien het buitengewoon eenvoudige karakter van de zaak.

https://bit.ly/2WLGM2s

Rechtbank Amsterdam 12 april 2019
(Overdragen domeinnaam)
Het bedrijf NewFysic voert een onderneming die zich bezighoudt met de exploitatie van een afslankmethode. Gedaagde doet hetzelfde en heeft op zeker moment een domeinnaam geregistreerd waar de handelsnaam van NewFysic deel van uitmaakt. Deze wordt ingezet als doorverwijzing, wat NewFysic niet zint. Partijen schikken hun geschil in 2010 met een onthoudingsverklaring voor dergelijk gebruik. Dit herhaalt zich in 2015 met een .be domeinnaam, en in een latere kwestie blijkt men de handelsnaam als magneetwoord in advertenties te gebruiken. De rechtbank komt tot het oordeel dat het boetebeding uit de onthoudingsverklaring uit 2010 is overtreden en er moet een stevige boete worden betaald. NewFysic blijkt dan weer een domeinnaam over de gedaagde te hebben, die moet worden afgedragen aan gedaagde wegens inbreuk op haar handelsnaamrecht.

https://bit.ly/2XPivdc

Rechtbank Limburg 17 april 2019
(Publicatie camerabeelden door gemeente)
Een journalist van dagblad De Limburger kon door omstandigheden meeluisteren met een vertrouwelijke raadsvergadering van de gemeente Kerkrade. De geluidsinstallatie bleek aan te staan en het geluid in de kamer ernaast ten gehore te brengen. De krant brengt bericht over een controversiële kandidaat-burgemeester, hetgeen tot ophef lijdt. De gemeente gaat na een vruchteloos strafrechtelijk traject over tot een persbericht waarbij beveiligingsbeelden worden gepubliceerd waarop te zien is hoe de journalist te werk ging. Volgens de journalist heeft de gemeente in de beelden geknipt en deze achter elkaar geplakt, waardoor een onvolledig en onjuist beeld van de feitelijke situatie ontstaat. De rechtbank is hard voor de gemeente: een dergelijke instantie moet zich van haar positie bewust zijn en zij dient te weten dat een burger bescherming verdient, met name tegen overheidsoptreden als het onderhavige. Zij moet weten dat indien een burger jegens haar beweerdelijk onrechtmatig handelt, de gang naar de rechter ook voor haar openstaat. In die rechtsgang kan zij schadevergoeding vorderen, indien zij van mening is dat een burger met het door de gemeente gestelde luistervinken onrechtmatig heeft gehandeld. Nu geen van de door de gemeente aangevoerde rechtvaardigingsgronden slagen, kan slechts worden

geconcludeerd dat de gemeente door de publicatie van de camerabeelden eigenrichting heeft gepleegd. Burger noch overheid mogen dat doen in Nederland.

https://bit.ly/31C4aTL

Rechtbank Amsterdam 18 april 2019
(Streamen van Eredivisie-voetbal)
Gedaagde exploiteert een café, en vertoont daar aan het bezoek Eredivisie-voetbal dat door FOX exclusief wordt uitgezonden. Dit doet zij eerst met licentie, maar na een betalingsachterstand van zo'n 3000 euro zegt ze deze op. Daarna blijkt zij toch door te gaan, en FOX ontdekt dit waarna een dwangsom van 1000 euro per uitzending wordt opgelegd.

https://bit.ly/2ZxJLO2

Rechtbank Oost-Brabant 24 april 2019
(Software-inbreuk)
Het bedrijf Planit exploiteert CAD/CAM software, waarmee industriële objecten kunnen worden ontworpen. Het bedrijf GTA heeft deze software met een aantal modules in licentie genomen. Op zeker moment rapporteert de software aan Planit dat een illegale kopie in gebruik is genomen, waarop Planit conservatoir beslag laat leggen en een rechtszaak wegens inbreuk start. De software blijkt gevirtualiseerd (middels VMware) aangeboden in het bedrijf, en blijkt bovendien een gekraakte versie. Dit is dan ook evident inbreuk. Dat men gelicentieerd was voor goeddeels dezelfde functionaliteit, doet daar niet aan af. De rechtbank komt uit op een kleine vijf ton schadevergoeding, ook al was deze software niet voor bedrijfsprocessen ingezet en was deze direct na ontdekking door de directie gewist.

https://bit.ly/2J18eEP

Rechtbank Amsterdam 13 mei 2019
(Naam van grensoverschrijdende hoogleraar)
Dagblad NRC publiceert onderzoeksjournalistiek waarin een hoogleraar arbeidsrecht aan de UvA wordt genoemd als pleger van diverse seksueel grensoverschrijdende feiten gedurende een lange periode en vanuit een stevige machtspositie. De rechtbank merkt de persoon aan als een zekere 'public figure' en gezien de ernst (en onderbouwing) van de feiten is het dan ook terecht dat NRC daarover publiceert. Echter, dit alles is volgens de rechtbank onvoldoende om hem met volledige naam (en mogelijk ook met foto) in het artikel te vermelden en daarmee (in de lengte der jaren, bijvoorbeeld door social media) aan de schandpaal te nagelen. Vooralsnog is, gezien de grote vlucht die de social media hebben genomen en alle commentaren die in de regel op uitingen van deze aard via internet te vinden zijn, voldoende aannemelijk gemaakt dat het noemen van zijn naam dergelijke gevolgen zal hebben. Van belang is ook dat NRC bekend staat als kwaliteitskrant, zodat de daarin vermelde zaken, zeker wanneer deze als feiten worden gepresenteerd, door een groot publiek voor 'waar' zullen worden gehouden.

https://bit.ly/2KodtBg

Rechtbank Zeeland-West-Brabant 17 mei 2019
(Phishing)
Verdachte werkte mee aan het verzenden van spam e-mails uit naam van de Rabobank. Indien slachtoffers vastliepen op de 'nep'website waar mensen naartoe werden geleid, belde verdachte uit naam van de Rabobank en loodste hen door het proces. Slachtoffers waren in de waan dat zij een nieuwe pinpas aanvroegen, maar in werkelijkheid zorgde verdachte er voor dat medeverdachte de beschikking kreeg over mobiel bankieren van het slachtoffer. Vervolgens werd er door medeverdachte een nieuwe pinpas aangevraagd, die door een verdachte werd afgevangen. Hierna werd de rekening van het slachtoffer, met gebruikmaking van moneymles, leeggehaald. Verdachte krijgt 5 jaar gevangenisstraf voor medeplegen van oplichting, computervredebreuk, diefstal en witwassen, allen meermalen gepleegd, deelname aan een criminele organisatie en valsheid in geschrifte.

https://bit.ly/2InBQx0

Rechtbank Noord-Nederland 21 mei 2019
(Domeinnaamfraude)
Het bedrijf Trademark Office (alleen die naam al) houdt zich bezig met domeinnaamdienstverlening, in het bijzonder het ongevraagd benaderen van bedrijven en hen erop wijzen dat iemand de .com versie van hun domeinnaam wil registreren. Er zou dan een waarschu-

wingsplicht zijn vanuit Trademark Office en men kan deze 'kaping' voorkomen door nu zelf de domeinnaam aan te vragen. Dit klinkt frauduleus en dat is het natuurlijk ook. 22 bedrijven stappen gezamenlijk naar de rechter. De kantonrechter komt tot het oordeel dat Trademark door het opzettelijk doen van onjuiste mededelingen deze bedrijven en personen heeft bewogen om een overeenkomst met Trademark te sluiten voor de registratie van de naam van hun website, maar dan met de extensie .com of .eu. en dat aldus sprake is van bedrog. De betreffende bedrijven en personen hebben de overeenkomst met Trademark gelet daarop terecht vernietigd. De kantonrechter veroordeelt Trademark in de volledige proceskosten, omdat zij naar het oordeel van de kantonrechter misbruik heeft gemaakt van procesrecht.

https://bit.ly/2MVRQuc

Rechtbank Noord-Holland 22 mei 2019
(Foto exwerknemer op bedrijfsbus)
Een oud-werknemer van een pakketbezorger constateert dat enkele bussen van de oud-werkgever nog steeds een foto tonen waarop hij zichtbaar werkt als bezorger bij het installeren van een bezorgde televisie. Tijdens het dienstverband heeft hij meegewerkt aan het maken van de foto, maar onduidelijk is wat precies de daarna verleende toestemming is. De werkgever heeft hierbij de bewijslast maar kan geen adequaat bewijs aandragen. De kantonrechter overweegt dat, als het gaat om gebruik van een portret zonder toestemming in een reclame-uiting, nog steeds de leer van het Discodanser arrest uit 1997 geldt, namelijk dat de geportretteerde in beginsel steeds een redelijk belang zal hebben om zich te verzetten tegen gebruik van zijn portret ter ondersteuning van een commerciële reclame-uiting. De geportretteerde zal door het publiek immers geassocieerd worden met het betreffende product of de dienst. Na enig geharrewar over de schade schat de rechter deze op 5.000 euro, in combinatie met een verbod en eis de foto onmiddellijk niet meer te gebruiken. Zie de noot op pagina 32.

https://bit.ly/2Fg2dmj

Rechtbank Den Haag 28 mei 2019
(Examens zijn persoonsgegevens)
Een student bij een Haags instituut slaagt niet voor zijn examens en verlaat de opleiding. Daarna wil hij op grond van de AVG inzage in zijn examens en beoordeling. De rechtbank in kort geding erkent dat deze gegevens persoonsgegevens zijn, en wijst het verzoek op inzage en kopie – gratis – toe.

https://bit.ly/2MR5Y89

Jorien Zwaneveld
Juridisch adviseur

Cloud | Contracteren | Overheid

De parodie als uitzondering op de Auteurswet

Het is algemeen bekend dat het niet is toegestaan om zomaar andermans werk geheel of gedeeltelijk te kopiëren zonder toestemming van de maker. Toch worden inbreuken op het auteursrecht op grote schaal gemaakt, door het bijvoorbeeld natekenen van tekeningen of het overschrijven van andermans teksten. Maar wat als iemand de spot wil drijven met een politicus door hem af te beelden als stripfiguur? Mag iemand voor de grap tekeningen van kinderboeken overnemen en teksten over drugs en hardcorefeesten erbij zetten?

De noodzaak van art. 18b Auteurswet

De wetgever wilde dat met art. 18b Auteurswet (hierna: Aw) 'het juiste evenwicht tussen rechthebbenden en gebruikers wordt bereikt.' Het is namelijk gezien de vrijheid van meningsuiting niet passend om met een beroep op het auteursrecht een karikatuur of parodie te dwarsbomen. Daarbij wordt de opmerking gemaakt dat de maker van een parodie, karikatuur of pastiche met een beroep op art. 18b Aw zich niet kan vrijwaren van verantwoordelijkheid en aansprakelijkheid: het beledigen van anderen, ook al kan een geslaagd beroep worden gedaan op art. 18b Aw, is nog steeds niet toegestaan. Er wordt door de wetgever dus een balans gezocht tussen de vrijheid van meningsuiting van de gebruiker en de gebruikersrechten van de maker van het oorspronkelijke werk.

De definitie van 'parodie' volgens het huidige recht

Mag je voor de parodie karakters natekenen of afbeeldingen overnemen? In 1984 oordeelde de Hoge Raad dat een vergaande mate van nabootsing van het oorspronkelijke werk is toegestaan, indien en voor zover de nabootsing noodzakelijk is om het werk herkenbaar, en daarmee het parodiërend karakter van de parodie, duidelijk te maken.[1] Een (gedeeltelijke) nabootsing van het oorspronkelijke werk lijkt ook haast onvermijdelijk voor het maken van een parodie, gezien de betekenis van het woord 'parodie'. Volgens de Van Dale is een parodie namelijk 'een grappige nabootsing om iets bespottelijk te maken.'

Duidelijke verschillen ten opzichte van het origineel

Hoe ver mag de nabootsing gaan? Het Hof van Justitie heeft in Deckmyn geoordeeld dat een parodie bestaat uit de nabootsing van een bestaand werk, maar dat er *duidelijke verschillen* moeten zijn ten opzichte van het bestaande werk.[2] Dit was bijvoorbeeld niet het geval bij het verhaal over Tanja Grotter en de Magische Contrabas, het zogenoemde 'Russische zusje van Harry Potter'.[3] Het verhaal over Tanja Grotter bevatte - naast de aanzienlijke lijst overeenkomsten - wel degelijk verschillen ten opzichte van Harry Potter en de Steen der Wijzen, bijvoorbeeld andere namen, een andere plaats waar het verhaal zich afspeelde, het gebruik van (Russische) mythologische figuren en het kunnen vliegen op stofzuigers. De verschillen waren echter zo minimaal dat de *totaalindruk* van de boeken door de ver-

1. HR 13 april 1984, ECLI:NL:HR:1984:AG4791, m.nt. L. Wichers Hoeth (*Vandersteen/Scriptoria*).
2. HvJ EU 3 september 2014, C-201/13, ECLI:EU:C:2014:2132 (*Deckmyn/Vandersteen*).
3. Hof Amsterdam 6 november 2003, ECLI:NL:GHAMS:2003:AN7646 (*Byblos/Rowling c.s.).*

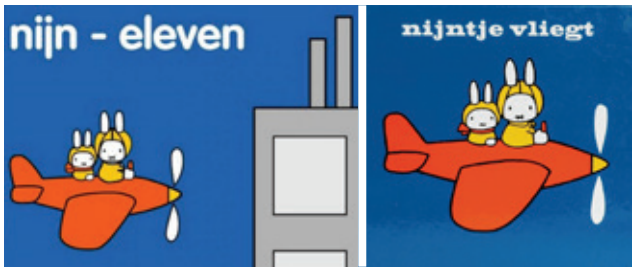
schillen niet anders werd. Het verhaal leek nog zo op dat van Harry Potter dat het overduidelijk een inbreuk op het auteursrecht was. Het gerechtshof noemde de verschillen zelfs gekunsteld en een mislukte poging om een eigen oorspronkelijkheid te geven aan het verhaal. De verschillen moeten dus wel groot genoeg zijn om daadwerkelijk onderscheidend te zijn.

Humoristisch bedoeld

Ten tweede is het vereist dat in de parodie de spot wordt gedreven of dat de parodie humoristisch bedoeld is. Het Hof van Justitie heeft in Deckmyn ook expliciet genoemd dat de parodie niet zo hoeft te verschillen van het oorspronkelijke werk dat het een eigen oorspronkelijk karakter krijgt, waardoor de parodie zelf beschermd wordt door de auteurswet. De parodie hoeft ook niet de spot te drijven met het oorspronkelijke werk of met de maker ervan. Tot slot is het niet vereist dat de bron wordt vermeld van het oorspronkelijke werk.

Ter illustratie: Nijntje

De verschillen tussen het oorspronkelijke werk en de parodie kunnen dus minimaal zijn, zolang er duidelijke verschillen bestaan en de parodie humoristisch bedoeld is. Een mooi voorbeeld van parodiërend gebruik met minimale verschillen biedt het arrest Bruna/Punt.nl, ook wel bekend als het Nijntje-arrest.[4] Punt.nl had een zevental afbeeldingen op haar websites staan waarop (een aangepaste tekening van) Nijntje te zien was, gecombineerd met teksten en beelden die niet bij Nijntje horen, bijvoorbeeld Nijntje op een hardcore feest, 'stoned als een garnaal', als 'trancenicht' en 'nijn-eleven'.



Links: nijn-eleven. Rechts: cover van het boekje 'nijntje vliegt' van Dick Bruna. Afbeeldingen via boek9.nl en bol.com.

In het geval van 'nijn-eleven' is een afbeelding van Nijntje letterlijk gekopieerd, maar is een tekst en getekend flatgebouw aan de afbeelding toegevoegd. Het gerechtshof oordeelde dat het hier ging om evident parodiërend gebruik. De spot lag er volgens het hof dik bovenop, en

4. Hof Amsterdam 13 september 2011, ECLI:NL:GHAMS:2011:BS7825, m.nt. M.H. Speyart.

door het toevoegen van het flatgebouw en de tekst is voldoende afstand tot het origineel genomen met behoud van herkenbaarheid van het origineel. Het hof voegde over de humoristische bedoeling nog toe dat het niet nodig is dat iedereen om de parodie kan lachen. Het arrest biedt een goed voorbeeld van hoe minimale wijzigingen aan het oorspronkelijke werk als overduidelijk parodiërend kunnen worden beschouwd en beschermd worden door art. 18b Aw.

Wanneer de parodie in het maatschappelijk verkeer geoorloofd is

Wanneer aan de vereisten voor het zijn van een parodie is voldaan, dan is het nog onzeker of de parodie geoorloofd is. Art. 18b Aw vereist immers dat een parodie geen inbreuk maakt 'mits het gebruik in overeenstemming is met hetgeen naar de regels van het maatschappelijk verkeer redelijkerwijs geoorloofd is.' Wanneer is dat het geval?

Evenwicht in belangen

Een parodie is in het maatschappelijk verkeer geoorloofd als er een rechtvaardig evenwicht bestaat tussen de belangen van de maker van het oorspronkelijke werk, en de vrijheid van meningsuiting van de maker van de parodie. Daarbij moet rekening worden gehouden met alle omstandigheden van het geval. Gaat de boodschap van de parodie veel verder dan de spot drijven, kritisch zijn of iets humoristisch uitbeelden, dan is de kans groot dat een beroep op art. 18b Aw faalt. Dit is het geval wanneer er bijvoorbeeld wordt gediscrimineerd, beledigd of haat wordt gezaaid.

Wat mag dan nog wel? Daarover schrijft Volgenant in de Groene Serie Onrechtmatige daad (2017) het volgende. Provoceren, irriteren en stijlvormen, zoals grof taalgebruik en straattaal-achtige bewoordingen, vallen onder de vrijheid van meningsuiting ex art. 10 EVRM. Daarnaast heeft het EHRM geoordeeld dat in sommige omstandigheden de vrijheid van meningsuiting door het gebruik van parodieën of satires extra waarde toekomen. Dit met name bij verkiezingen, een situatie waarin verkiezingskandidaten meer moeten kunnen verdragen. Bij het maken van parodieën en satires is ook het betrekken van staatshoofden tot op zekere mate geoorloofd.

Voor het parodiërend gebruik maakt het tevens niet uit dat de maker van het oorspronkelijke werk zich beledigd voelt door de parodie. Zijn aan de voorwaarden van een parodie voldaan, dan is er geen sprake van 'misvorming, verminking of andere aantasting van het werk' ex art. 25 lid 1 sub d Aw waar de maker van het oorspronkelijke werk zich tegen kan verzetten. Is iets een parodie, dan is het 'niets meer dan een parodie', blijkt uit Bruna/Punt.nl.

Verwarringsgevaar

Verder is voor de geoorloofdheid in het maatschappelijk verkeer van belang of het normale publiek het origineel met de parodie zou kunnen verwarren. Dit verwarringsgevaar komt eigenlijk neer op de eerder genoemde eis van Deckmyn voor het duidelijk verschillen van het oorspronkelijke werk. Het moet voldoende duidelijk zijn dat het gaat om een parodie, een humoristische nabootsing van het origineel.

Samengevat

Een parodie is een nabootsing van een bestaand werk met duidelijke verschillen, die humoristisch bedoeld is. De parodie hoeft geen eigen oorspronkelijk karakter te hebben, en het hoeft ook niet de spot te drijven met het oorspronkelijke werk of de maker van het werk. Ook de bron van het oorspronkelijke werk hoeft niet vermeld te worden.

Wanneer het gebruik van een parodie in het maatschappelijk verkeer geoorloofd is, hangt af van alle omstandigheden van het geval. Er wordt een rechtvaardig evenwicht gezocht tussen de belangen van de maker van het oorspronkelijke werk en de vrijheid van meningsuiting van de maker van de parodie. Belangen die mee kunnen spelen zijn verwarringsgevaar, het ontbreken van concurrentiebedoelingen, de omstandigheden waarin de parodie tot stand is gekomen en de boodschap van de parodie.

ICTRECHT
adviesbureau

Een passende escrow of continuïteitsoplossing voor uw organisatie nodig?

Maakt u gebruik van software of clouddiensten die bedrijfskritisch zijn voor uw organisatie? Heeft u nagedacht over wat er gebeurt als uw leverancier failliet gaat? Weet u of u dan nog wel kunt voldoen aan uw wettelijke bewaarplichten? ICTRecht biedt oplossingen op het gebied van escrow en continuïteit, voor zowel gebruikers als aanbieders van software en clouddiensten. Voor elke situatie gaan wij in overleg met u op zoek naar de best werkbare oplossing.

Mogelijke oplossingen zijn onder meer:

Software en SaaS escrow

Notariële escrow

Verificaties van broncodes

Continuïteit in de cloud

Overdragen, splitsen of verpanden van auteursrechten

Second opinions

Wilt u meer weten over deze dienst?

Meer informatie is te vinden op: ictrecht.nl/escrow.
Of vraag een kennismakingsgesprek aan via telefoonnummer:
020 663 1941 (ICTRecht Amsterdam) of 050 209 3499 (ICTRecht Groningen).
Ons een e-mail toesturen kan ook via: escrow@ictrecht.nl

Arnoud Engelfriet
Algemeen directeur /
Opleidingsdirecteur

Noot bij Rechtbank Noord-Holland 22 mei 2019

(Foto ex-werknemer op bedrijfsbus)

Tot hoe lang na uitdiensttreding mag je als werknemer worden ingezet als 'gezicht' van het bedrijf? Die vraag stond centraal in een conflict tussen een oud-werknemer van een pakketbezorger en de werkgever. De werkgever werkt als onderaannemer voor PostNL Extra@Home, de speciale bezorgdienst voor grotere producten van PostNL waarbij ook een installatieservice kan worden afgenomen. Om dat te illustreren, had men een mooie foto gemaakt van twee installateurs bezig met het afleveren van een televisie:

Foto uit vonnis (fotograaf niet genoemd bij origineel)

Deze foto werd gebruikt bij persberichten over de dienst, maar op zeker moment ook aangebracht als foto op bezorgbussen en vrachtwagens. Daar maakte de persoon links bezwaar tegen, omdat hij inmiddels uit dienst was en niet meer met deze werkgever geassocieerd wilde worden.

In eerste instantie verliep de discussie minnelijk: hij vroeg een vergoeding voor gebruik van zijn portretrecht, en het bedrijf onderhandelde daar zakelijk over, maar de discussies liepen na geruime tijd spaak. Enkele jaren later pakte de man het opnieuw aan via een advocaat, waarna de werkgever aangaf dat er al geschikt was en dus niets meer betaald hoefde te worden. Daarop stapte de man naar de rechter voor een verbod met schadevergoeding.

Uitgangspunt van de man was dat de foto's specifiek waren gemaakt voor intern gebruik ten behoeve van een presentatie aan medewerkers over een nieuwe bedrijfstak van de werkgever en niet voor de promotionele of commerciële doeleinden waarvan in het onderhavige geval sprake is. De werkgever stelde daar tegenover dat hij als werknemer toestemming had gegeven voor het gebruik van zijn beelden, zonder dat er aan die toestemming beperkingen waren verbonden. Met dat stuk is de rechter snel klaar: er was geen duidelijk bewijs van toestemming, met name was er geen ondertekend stuk.

De rechtbank gaat vervolgens verder op het 'redelijk belang' uit het portretrecht (artikel 21 Auteurswet). Dit doet wat vreemd aan anno 2019, nu een foto een persoonsgegeven is en de AVG daarop van toepassing

is. De AVG vervangt daarmee het klassieke portretrecht, omdat Europees recht immers nationaal recht vervangt. Maar allereerst dateert het gebruik van de foto van vóór de AVG, en ten tweede roept de man geen privacygrondslag in voor zijn argument: hij maakt bezwaar tegen de associatie met het bedrijf, hij wil niet langer het 'gezicht' van deze dienstverlening zijn. Dat is een aparte grond, los van de privacy.

Deze grond is al in 1997 apart erkend in het Discodanser-arrest (HR 2 mei 1997, ECLI:NL:HR:1997:-ZC2364, NJ 1997, 661). De Hoge Raad formuleerde hierin de norm dat een geportretteerde in beginsel steeds een redelijk belang zal hebben om zich te verzetten tegen gebruik van zijn portret ter ondersteuning van een commerciële reclame-uiting. De geportretteerde zal door het publiek immers geassocieerd worden met het betreffende product of de dienst, waarbij het publiek in het algemeen - en doorgaans terecht - ervan uit zal gaan dat het gebruik van het portret niet zal zijn geschied zonder toestemming van de geportretteerde en de opname van het portret in de reclame-uiting zal opvatten als een blijk van publieke ondersteuning van het product of de dienst door de geportretteerde. Op deze gronden is het op een dergelijke wijze gebruiken van een portret in beginsel aan te merken als een inbreuk op de persoonlijke levenssfeer van de geportretteerde (strijd met artikel 8 EVRM).

In theorie is het mogelijk om die inbreuk te rechtvaardigen met beroep op een ander grondrecht. Dit zal meestal de uitingsvrijheid (artikel 10 EVRM en artikel 7 Grondwet) zijn. In dit geval is dat niet sterk, het gaat om een reclame-uiting en geen redactionele boodschap. Daarbij is niet van belang of de foto's al dan niet schadelijk zouden zijn voor zijn reputatie en/of dat de werknemer een verzilverbare populariteit geniet of niet. Bovendien had de werkgever dit niet nader onderbouwd.

Blijft over de beweerdelijke afkoopregeling. Deze gaat de mist in omdat de werkgever namens hem heeft onderhandeld met PostNL, maar geen bevoegdheid daartoe had. Zelf heeft hij niet ingestemd met deze regeling. Ook gezien het geringe bedrag (480 euro, tegen eisers eerdere eigen vergoeding van 10.000) mocht hier geen bevoegdheid worden aangenomen.

De schadevergoeding voor een kwestie als deze is natuurlijk altijd lastig. De rechtbank schat haar op 5.000 euro, rekening houdend met de prominente plaats van de foto van het portret van eiser op de transportmiddelen en het voorkomen van beelden van hem in een reclamefilmpje, dat nog steeds op het internet is te vinden. Dat voelt stevig, maar is wel terecht ook gezien het lange traject en het gemak waarmee de werkgever dit had kunnen voorkomen.

Welke lessen zijn hier nu uit te trekken? Allereerst natuurlijk dat je als werkgever duidelijke afspraken moet maken én op papier moet zetten. Daarbij zal al snel het argument te berde komen dat onder de AVG werknemers geen toestemming kunnen geven, vanwege het ontbreken van het 'vrije' karakter vanwege de afhankelijkheidsrelatie tot de werkgever. Dit vonnis danst daar mooi omheen: het gaat om een niet-persoonsgegevens gerelateerde kwestie, namelijk het commercieel portretrecht. Daarbij staat een belangenafweging voorop, en toestemming is een factor binnen de belangen die moeten worden afgewogen. De mate van vrijheid bij die toestemming kan daarin worden meegenomen, maar is niet in zijn eentje doorslaggevend.

Wel denk ik dat in het algemeen het ophoudt zodra de werknemer uit dienst gaat. Het kan niet waar zijn dat een werkgever goede sier blijft maken met een foto van een ex-werknemer. Zo dat al niet volgt uit privacy of portretrecht, zal het toch volgen uit gewoon de open norm van goed werkgeverschap. Zoiets doe je niet. (Eventuele historische documenten zoals oude brochures of een reeds gepubliceerd filmpje met datum daargelaten.) Als werkgever zul je dus altijd een plan paraat moeten hebben om dergelijke uitingen te vervangen wanneer de gefilmde werknemers uit dienst gaan.

Van onze blog

Privacy | E-commerce | Innovatie | Marketing | Overheid

1 mei 2019

Voldoen aan privacywetgeving: het levert je organisatie voordelen op

Het voldoen aan de privacywetgeving is meer dan een tijdrovende ballast: het kan je bedrijf positief beïnvloeden. En dan hebben we het niet alleen over een schoon geweten en een verminderd financieel risico qua boetes en overige aansprakelijkheden. Uit onderzoek blijkt namelijk dat het voldoen aan de privacywetgeving ook goed is voor je business. Door de juiste privacymaatregelen te treffen, ervaren organisaties voordelen, zoals: minder datalekken en minder verkoopvertragingen. Daarnaast heb je als privacyproof organisatie een streepje voor als het op concurrentie aankomt, aldus recent onderzoek van Cisco. In deze blog bespreken we de resultaten van dit onderzoek naar de positieve gevolgen van het voldoen aan de AVG.

Internationaal onderzoek onder beveiligings- en privacy professionals

Bovengenoemde positieve effecten van het voldoen aan de privacywetgeving, komen voort uit de in januari van dit jaar gepubliceerde Cisco 2019 Data Privacy Benchmark Study[1], die is gebaseerd op resultaten uit een survey afgenomen onder 3.200 beveiligings- en privacy professionals uit 18 landen. Organisaties die hebben geïnvesteerd om zich op de Algemene Verordening Gegevensbescherming (AVG) voor te bereiden, hebben dit in eerste instantie gedaan om te ontkomen aan de aanzienlijke boetes en andere straffen die gelinkt zijn aan het niet voldoen aan de AVG. Echter, uit het onderzoek blijkt dat er nog andere aantrekkelijke voordelen verbonden zijn aan het doen van investeringen op het gebied van privacy. Deze leggen we hieronder verder uit.

Minder vertraging in de verkoopcyclus

Steeds meer mensen lijken hun privacy serieus te nemen. Volgens de Autoriteit Persoonsgegevens[2] zou maar liefst 94% van de Nederlanders zich zorgen maken over de bescherming van zijn persoonsgegevens. In het Cisco-onderzoek werd gevraagd of de professionals vertragingen in hun verkoopcyclus ervaren als gevolg van het toegenomen bewustzijn over privacy. Het merendeel van de bedrijven (87%) antwoordde hier bevestigend op. Een aanzienlijke stijging ten opzichte van de 66% in de survey van vorig jaar[3]. Daarnaast ondervonden bedrijven die het minst voldeden aan privacywetgeving bijna 60%(!) meer vertraging in hun verkoopcyclus (5,4 versus 3,4 weken). Volgens de bedrijven hebben de vertragingen vooral te maken met het voldoen aan de privacyvereisten van de klant en deze op een duidelijke wijze informeren over hun privacybeleid.

Minder kostbare datalekken

Een ander voordeel is de vermindering van de frequentie en impact van datalekken. Bedrijven die het meest voldeden aan de AVG hadden het afgelopen jaar minder kans op een datalek (74%) dan bedrijven die het minst compliant waren (89%). Minder persoonsgegevens waren getroffen (79.000 versus 212.000). Indien sprake was van een systeemuitval was deze van kortere duur (6.4 uur versus 9.4 uur) en slechts 37% van deze bedrijven leed aan verliezen van ten minste 500.000 dollar. Dit ten opzichte van 64% van bedrijven die het minst waren voorbereid.

Last but not least zijn datalekken op zijn zachtst gezegd slecht voor klantvertrouwen. Uit onderzoek[4] van de Britse betalingsbeveiligingsfirma PCI Pal is

1. https://bit.ly/2Mvse3D
2. https://bit.ly/2B42VB6
3. https://bit.ly/2DKZCCe
4. https://bit.ly/2X5DMOK

gebleken dat 44% van consumenten zich enkele maanden zou onthouden van het doen van aankopen en 41% definitief zou stoppen met het bezoeken van een winkel naar aanleiding van een datalek.

Bijkomende voordelen van voldoen aan de AVG
Volgens het Cisco-onderzoek geven de meeste bedrijven (97%) aan dat ze bijkomende voordelen genieten uit hun investeringen die verder gaan dan alleen voldoen aan de nalevingsvereisten. Deze omvatten onder meer het hebben van een concurrentievoordeel, aantrekkelijk zijn voor investeerders, operationele efficiëntie en ruimte voor flexibiliteit en innovatie. Driekwart van respondenten zegt twee of meer voordelen te genieten. Bovendien is de meerderheid van alle bedrijven van mening dat een goed privacybeleid een sterk onderscheidende factor is op de markt.

Deze resultaten benadrukken dat organisaties niet alleen veranderingen zouden moeten doorvoeren om te voldoen aan de vereisten van privacywetgeving, maar ook om de zakelijke voordelen van hun investeringen te maximaliseren. Dus maak de privacy medewerkers, juristen, FG's en overige privacy champions (of hoe je ze ook noemt) eens blij en vraag niet naar de risico's rondom de privacywetgeving, maar naar alle voordelen die het je organisatie oplevert, want dat kunnen er dus nogal wat zijn!

Deze blog is geschreven door stagiaire Ge'ez Engidashet, in samenwerking met Michelle Wijnant.

Auteur
Michelle Wijnant
Juridisch adviseur

29 mei 2019

De AVG in het onderwijs: hebben scholen hun huiswerk gedaan?

De invoering van de AVG heeft flinke gevolgen gehad voor scholen in het primair en voortgezet onderwijs. Het is dan ook logisch dat er bij bestuurders, leraren en onderwijsondersteunend personeel veel vragen leven rondom de omgang met persoonsgegevens van leerlingen. Waar moet je als school nu op letten voor een privacyvriendelijke onderwijsomgeving? En hoe zorg je dat leraren en onderwijsondersteunend personeel ongehinderd hun werk kunnen doen en toch veilig omgaan met persoonsgegevens?

De basis: doelbinding en dataminimalisatie
Als uitgangspunt van alle verwerkingen van persoonsgegevens geldt: bepaal allereerst voor welk doel je ze wil (of moet) gebruiken. Zodra je ze voor een specifiek doel hebt ontvangen, gebruik ze dan ook alleen daarvoor. Toetsresultaten moet de school bijhouden om de voortgang van een leerling bij te houden, maar men mag ze niet zomaar aan een bijlesinstituut verstrekken. Een foto die oorspronkelijk – met toestemming – gemaakt is voor in de schoolgids mag niet zomaar op Instagram worden gepubliceerd.

Aanverwant aan het begrip doelbinding is het principe van dataminimalisatie. Niet alleen mag je gegevens alleen voor het vooraf bepaalde doel gebruiken, gegevens die niet (meer) strikt nodig zijn mogen niet worden bewaard. Wees dus bij het verzamelen van persoonsgegevens kritisch welke noodzakelijk zijn en hanteer bewaartermijnen zodat persoonsgegevens die overbodig zijn, worden gewist.

Zodra dit alles intern op orde is, kan (en moet) de school het beleid uitleggen aan leerlingen en ouders. Op deze manier wekt de school vertrouwen dat op een weloverwogen en veilige manier met de persoonsgegeven van de leerlingen wordt omgegaan.

Toestemming
Veelal zijn persoonsgegevens die scholen beheren nodig voor het uitvoeren van de wettelijke taak: het verzorgen van onderwijs. Scholen hebben echter ook regelmatig behoefte aan gegevens voor andere doeleinden. Denk aan beeldmateriaal voor promotiedoeleinden of om verslag te doen van activiteiten. Ook het publiceren van een lijst van geslaagden[1] in de lokale krant is een voorbeeld wat veel discussie losmaakt.

Voor veel verwerkingen van persoonsgegevens buiten de wettelijke taken, zoals de situaties hierboven, is volgens de Autoriteit Persoonsgegevens (AP) toestemming nodig. Die toestemming geeft de leerling zelf als deze 16 jaar of ouder is, anders is toestemming van een ouder of voogd nodig. Een verklaring van toestemming onder de AVG moet kunnen worden aangetoond: verkrijg deze dus altijd schriftelijk. Daarnaast moet de toestemming specifiek zijn - toestemming voor een foto in de schoolgids geldt dus niet voor andere soorten van publicatie. Ten slotte dient de toestemming met een vrije, actieve handeling te zijn gegeven: “als je geen bezwaar maakt ga je akkoord met …” is dus niet de juiste manier.

Functionaris Gegevensbescherming
Scholen zijn verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. De FG ziet toe op een correcte naleving van het de AVG en het informatiebeveiligings- en privacybeleid (IBP-beleid) en adviseert het bestuur over te nemen maatregelen. Deze functionaris hoeft niet in dienst te zijn. Het hoeft ook geen fulltime rol te zijn. Een FG op afstand is voor veel scholen daarom een goede oplossing. Bij één op de drie scholen in het PO en één op de tien scholen in het VO is nog geen FG aangesteld[2].

Implementatie IBP-beleid
Volgens onderzoek in opdracht van Kennisnet[3] zijn 75% van de PO-scholen en 84% van de VO-scholen goed op weg of zelfs al klaar met het IBP-beleid. Dat

1. https://bit.ly/2J5M4RN
2. https://bit.ly/2YbsqtD
3. https://bit.ly/2TWjHOh

zijn hoopvolle cijfers. Ook op het gebied van datalekken lijkt het in het onderwijs relatief goed te gaan. In 2018, het eerste jaar waarin de AVG van kracht was, was 3% van de meldingen van datalekken[4] die de Autoriteit Persoonsgegevens ontvangen heeft, afkomstig vanuit het onderwijs.

Toch kunnen scholen niet stilzitten. Het IBP-beleid moet ook in concrete actie worden omgezet. Er moet blijvend worden gewerkt aan bewustwording onder medewerkers. Ook de maatregelen om systemen en persoonsgegevens te beveiligen hebben doorlopend aandacht nodig. Om scholen te ondersteunen bij het samenstellen en uitvoeren van een goed privacybeleid is de Aanpak IBP[5] in het leven geroepen. Dit programma wordt ondersteund door Kennisnet, de PO-raad en de VO-raad. Het is recent vernieuwd en biedt praktische hulp aan scholen bij het implementeren van een gedegen privacybeleid.

4. https://bit.ly/2YmM6v3
5. https://bit.ly/2KCL8aL

De ervaring leert dat het prima mogelijk is om een privacybeleid door te voeren, terwijl leraren en ander personeel zich nog gewoon kunnen bezighouden met waar zij goed in zijn. Het implementeren van een IBP-beleid beantwoordt veel vragen die leven op de werkvloer en schept kaders voor de omgang met persoonsgegevens. Die kaders helpen om iedereen het vertrouwen te geven dat de persoonsgegevens binnen de school in veilige handen zijn.

Auteur
Dimmen Smolders
Juridisch adviseur

Trainingsoverzicht september 2019 – oktober 2019

Voor juridische professionals

Donderdag 5 september 2019

Technologie: werking internet II (4PO)
Technische kennis stelt de ICT-jurist in staat om de vertaalslag te maken van het juridische naar het technische en vice versa. In de huidige tijd waarbij ICT grotendeels online wordt geleverd, is kennis van de werking van het internet daarbij cruciaal.

https://bit.ly/2EiXXCJ

Dinsdag 10 september 2019

Cloud en software: beschikbaarheid van clouddiensten (4PO)
Outsourcing naar de cloud brengt enorme afhankelijkheid mee. Gebruikers van clouddiensten moeten daarom altijd afspraken maken over beschikbaarheid. Verlies van data of dienst kan immers leiden tot bedrijfsdiscontinuïteit. Daarbij wordt onderscheid gemaakt tussen tijdelijke onbeschikbaarheid en definitieve onbeschikbaarheid. De eerste situatie kan met een goede service level agreement (SLA) worden opgevangen, de tweede vereist exit- of continuïteitsafspraken.

https://bit.ly/2TUcB8M

Dinsdag 17 september

Privacy en persoonsgegevens: verwerkersovereenkomst (4PO)
De verwerkersovereenkomst is de juridische borging in de relatie tussen een verantwoordelijke en een verwerker in de omgang met persoonsgegevens. Vaak wordt hierbij een standaarddocument gebruikt, de uitdaging is dit te laten aansluiten bij de werkelijke situatie en de daarnaast bestaande documenten zoals SLA of licentieovereenkomst.

https://bit.ly/2EeNfy3

Donderdag 19 september

Cloud en software: softwarerecht (4PO)
Om te kunnen adviseren over cloud en software moet de ICT-jurist software kunnen kwalificeren en bekend zijn met de relevante wetten en de contractspraktijk. De ICT-jurist moet creatief zijn en wetten en regels vertalen, zodat ze zoveel mogelijk toepasbaar blijven op voortschrijdende technologie.

https://bit.ly/2ASguRb

Dinsdag 24 september

Privacy en persoonsgegevens: de basis (6PO)
In deze dagtraining wordt de AVG op hoofdlijnen uitgewerkt om zo het kader voor een zorgvuldige omgang met persoonsgegevens te kunnen realiseren.

https://bit.ly/2s4yA12

Donderdag 26 september

Contracteren: de basis (6PO)
Contracteren ligt aan de wortel van een groot deel van het ICT-recht. ICT-contracten kennen verschillende types, van softwarelicentie tot resellerovereenkomst en van algemene voorwaarden tot mantelcontract. Elk contract vereist algemene aandachtspunten en daarnaast specifieke aspecten.

https://bit.ly/2rjRy19

Dinsdag 8 oktober

Privacy en persoonsgegevens: de verdieping (6PO)
Privacywetgeving kent open normen en grijze gebieden. Als jurist moet u deze kunnen identificeren en op een deskundige en begrijpelijke wijze naar de praktijk kunnen vertalen. Tijdens de training leert u onder meer over binding corporate rules, de verwerkersovereenkomst, registers en de Functionaris Gegevensbescherming (FG).

https://bit.ly/2rk8VPi

Donderdag 10 oktober

Privacy en persoonsgegevens: omgang met datalekken (4PO)
Datalekken en misbruik van persoonsgegevens staan hoog op de agenda gezien de recente wetgeving hierom-

trent. De senior jurist moet hierin kunnen adviseren, zowel in omgang met ontstane lekken alsook in het voorkomen van toekomstige lekken.

https://bit.ly/2Xkdn0y

Voor algemeen publiek

Donderdag 12 september

Update Algemene Verordening Gegevensbescherming (AVG)

Wij praten u in een middag bij over de belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming (AVG), met zich mee heeft gebracht. Over hoe u onder de AVG moet omgaan met persoonsgegevens, beveiliging en datalekken, en wanneer een Functionaris Gegevensbescherming (FG) verplicht is.

https://bit.ly/2UfAf06

Donderdag 3 oktober

Privacy & de AVG in het arbeidsrecht

Ook op gegevens verwerkt in de arbeidsomgeving is de privacywetgeving uit de AVG van toepassing. In deze training behandelen wij de relevante regels uit de AVG en het arbeidsrecht in het kader van de omgang met medewerkersgegevens. Daarnaast bespreken we onderwerpen die in de werkgevers/werknemersverhouding nogal eens tot discussies leiden, zoals de omgang met social media uitingen van medewerkers en het gebruiken van informatie over zieke medewerkers.

https://bit.ly/2HOWdTv

ICT en Gezondheidsrecht

Dinsdag 1 oktober

ICT & zorg: contracteren in de zorg (algemeen en specifiek)

Binnen de zorg wordt op grote schaal geïnnoveerd en gedigitaliseerd. Wij nemen u in deze eerste twee bloktrainingen mee door de juridische aspecten bij toepassing van ICT in de gezondheidspraktijk. In de eerste bloktraining bespreken we onder meer welke ICT-oplossingen u tegenkomt in de zorg. In de tweede training gaan we in op zorg-administratiesystemen, eHealth applicaties voor het online verlenen van zorg, platforms voor het kopen van zorgproducten en zorgfora.

https://bit.ly/2BIxywc

FG / DPO training

Binnen onze FG-opleiding onderscheiden wij diverse trainingsdagen (de zogeheten themadagen). Op een themadag wordt één specifiek thema behandeld en zijn ook los afneembaar.

Donderdag 5 september - FG en privacywetgeving
Donderdag 19 september - Soft skills
Donderdag 26 september - Verantwoordelijke en verwerker deel I*
Donderdag 3 oktober - Verantwoordelijke en verwerker deel II*
Donderdag 10 oktober - Security

*Deze themadag beslaat twee dagen. Om aan deel II te mogen deelnemen, dient deel I gevolgd te zijn.

ictrecht.nl/opleiding-fg-dpo

Heeft u vragen of wilt u meer weten?
Neem dan contact op met onze opleidingscoördinator Alisa Schurink via e-mail: academy@ictrecht.nl of telefoonnummer: 020 663 19 41.

Alisa Schurink
Opleidingscoördinator
en Marketingmedewerker


ICTRECHT
adviesbureau