MAY 2017

Mr. V.A. DE POUS

A TREND ANALYSIS

Juridische trends in digitale transformatie

Deze studie wordt aangeboden door de
Stichting Cloud Community Europe Nederland

Key issues

- Van chartaal geld naar elektronisch betalingsverkeer. Van papieren reisbewijs naar eTicket en OV-chipkaart. Van traditioneel handelen naar nieuwe manieren van plaats- en tijdonafhankelijk werken, zakendoen en besturen. De digitale transformatie is in volle gang. Algemeen beschouwd gaat het om de verandering in verband met de toepassing van digitale technologie in alle aspecten van onze samenleving. Gericht op verbetering: meer welvaart en welzijn.
- De actuele katalysator achter de transitie vormt het leveringsmodel voor digitale techniek en informatievoorziening *cloud computing* (gecentraliseerd), hoewel ook nieuwe modellen zich aandienen. Bij *edge computing* (gedistribueerd) worden gegevens verwerkt, in beginsel vlakbij waar ze ontstaan, hetgeen een uitermate geschikte modus operandi betreft voor Internet of Things-toepassingen. Op deze wijze wordt de digitale infrastructuur ontzien.
- De digitale verandering laat het recht niet onberoerd. De laatste 25 jaar hebben de Europese en Nederlandse wetgever een omvangrijk en tegelijkertijd divers legislatief pakket voor de informatiemaatschappij geïntroduceerd, waarvan het eind niet in zicht is. Sterker nog, er komt steeds meer wet- en regelgeving bij. Daar moet iedere onderneming of overheidsorganisatie rekening mee houden, los van de veranderingsfase, waarin zij zich bevindt. *Digitaal recht is Chefsache geworden*.
- Tenminste drie juridische clusters spelen een belangrijke rol bij digitalisering, te weten het recht met betrekking tot (i) elektronische identiteiten en vertrouwensdiensten, (ii) verwerking van persoonsgegevens en (iii) netwerk- en informatiebeveiliging, inclusief meldplichten voor ICT-gerelateerde incidenten, zoals datalek, veiligheidsinbreuk of verlies van integriteit.

Een veelbesproken verandering

Evenals voor het concept voor een slimme stad of nieuwe manieren van werken, ontbeert digitale transformatie een uniforme omschrijving of juridische definitie. Dat remt de praktijk geenszins, maar nodigt soms wel uit tot spraakverwarring. Wikipedia spreekt van een 'onderdeel van een groter technologisch proces en de verandering in verband met de toepassing van digitale technologie in alle aspecten van de menselijke samenleving'. Nader bepaald kan digitale transformatie worden gezien als

'*the third stage of embracing digital technologies: digital competence → digital usage → digital transformation, with usage and transformative ability informing digital literacy. The transformation stage means that digital usages inherently enable new types of innovation and creativity in a particular domain, rather than simply enhance and support the traditional methods*.'[1]

Papierloos

Een smallere focus noteren we ook. In engere zin verwijst digitale transformatie naar *de overgang naar een papierloos individueel bedrijf of overheidsorganisatie*, of naar een papierloze economische sector of ander collectief segment van de samenleving, zoals belastingheffing of openbaar bestuur. Snel ging dat niet, gelet op het feit dat het concept van het papierloze kantoor 40 jaar geleden opkwam.[2] Nu zijn talloze transities — eindelijk — in volle gang. Zo zet de Nederlandse regering zwaar in op de digitalisering van overheidsorganisaties, aldus de kabinetsdoelstelling Digitaal 2017; vooral in de relatie met burger en ondernemer.[3] Zowel (i) informatievoorziening door als (ii) transacties met een overheidsorganisatie worden in toenemende mate digitaal.

Informatievoorziening en transacties

Nog een voorbeeld. De Eerste Kamer stemde op 4 oktober 2016 in met een wetsvoorstel dat de elektronische uitwisseling van medische gegevens *tussen zorgverleners* regelt.[4] Of denk niet alleen aan papierloos procederen voor de rechter, maar tegelijkertijd proces-voering op afstand, via Internet.[5] Om digitale producten en diensten op een eenduidige, herkenbare en efficiënte manier aan burger en bedrijf aan te bieden, is het gebruik van zoiets als een generieke digitale infrastructuur van groot belang. Met deze generieke digitale basisvoorzieningen kunnen overheidsorganisaties hun digitale processen inrichten.

Hoe het ook zij, dat digitalisering niet zonder solide rechtskaders kan, laat zich raden.

[1] https://en.wikipedia.org/wiki/Digital_transformation

[2] Het Amerikaanse ICT-bedrijf Micronet, Inc. gebruikte in 1978 voor het eerst de term 'The Paperless Office'.

[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2016/12/15/aanbiedingsbrief-voortgangsrapportage-digitaal-2017

[4] Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens), 33.509.

[5] https://www.rijksoverheid.nl/onderwerpen/rechtspraak-en-geschiloplossing/inhoud/vernieuwing-in-de-rechtspraak/programma-kwaliteit-en-innovatie-rechtspraak-kei

Efficiëntie en innovatie — welvaart en welzijn

De ratio van digitalisering — kort gezegd, de toepassing van informatie- en communicatietechnologie in producten, diensten, werkprocessen en verdienmodellen — ligt voor de hand. De algemene notie luidt, dat de inzet van ICT de prestatie van individu, organisatie, keten of bedrijfstak, en samenleving als geheel, kan verbeteren. Hierbij gaat het zowel om de verdere ontwikkeling van meer traditionele vormen van ICT, zoals bedrijfssoftware in de vorm van enterprise resource planning (ERP) en customer relationship management (CRM), als ook om allerlei vernieuwing. Autonoom-handelende digitale systemen, het Internet of Things, zelflerende systemen en bijvoorbeeld verregaande robotisering zullen straks in veel sectoren ingang vinden.

Economie

Volgens de Nederlandse regering heeft digitalisering — mede — een 'fundamentele impact op de economie: het verandert bijvoorbeeld wat de economie produceert (nieuwe, gepersonaliseerde producten en diensten), de wijze van productie (smart industry, nieuwe verdienmodellen) en de organisatie (opkomst van digitale platforms, consument wordt producent) ervan. In de wetenschap gaat digitalisering hand in hand met de beweging naar Open Science: open toegang tot wetenschappelijke publicaties en onderzoeksgegevens. Digitalisering is daarmee een bron van innovatie, bedrijvigheid en economische groei. Bovendien biedt het nieuwe mogelijkheden voor de aanpak van maatschappelijke uitdagingen.'[6] Voor wat betreft de vernieuwing van de rechtspraak gaat het vooral om vereenvoudiging.

De nationale digitale agenda mag dan vooral een economische betreffen; van de analyse van grote hoeveelheden gegevens uit verschillende bronnen (big data) wordt bijvoorbeeld in de medische sector een andersoortige verbetering verwacht. Meer welzijn, door minder ziekten of door deze beter te bestrijden.

Product- en dienstontwikkeling

De overgang van analoog naar digitaal is niet met rozen geplaveid, zo weten onder meer uitgevers van boeken, tijdschriften en kranten. De digitale transitie tegenhouden is echter geen optie. Sommigen boeken meer vooruitgang dan anderen. Zo kent Het Financieele Dagblad het hoogste percentage digitale lezers van alle landelijke dagbladen in Nederland. Volgens de NOM-bereikcijfers over de periode tweede half jaar 2015 t/m eerste half jaar 2016 houdt de zakenkrant zijn sterke digitale groei vast. 33,4% leest enkel digitaal.[7]

De zaak Nike

Naast allerlei feitelijke drempels, constateren we juridische drempels en piketpalen. Wie als producent bij de ontwikkeling van een product of dienst onvoldoende oog heeft voor het dwingende rechtskader van digitale technologie, kan van rechter of toezichthouder lik op

[6] Kamerbrief 5 juli 2016 van de Minister van Economische Zaken.

[7] http://www.marketingtribune.nl/online/nieuws/2016/09/fd-koploper-in-digitale-transitie/index.xml

stuk krijgen. Zo informeerde Nike de gebruikers van de Nike+ Running app — die voor de goede orde miljoenen malen is gedownload — onvoldoende over de verwerking van hun gezondheidsgegevens. Nike verkrijgt daardoor ook niet de vereiste uitdrukkelijke toestemming van de app-gebruikers, aldus concludeerde onze privacytoezichthouder in 2015.[8] De Amerikaanse sportkledinggigant handelt in strijd met de Wet bescherming persoonsgegevens, doordat deze gebruikers onvoldoende informeert over dat via de app gezondheidsgegevens worden verwerkt. Hierdoor is geen sprake van geïnformeerde toestemming. Ook vertelt Nike de gebruikers niet, dat hun persoonsgegevens worden verwerkt voor analyse- en onderzoeksdoeleinden, bijvoorbeeld door gebruikers op basis van leeftijd, geslacht, ervaring en hardloopniveau in segmenten in te delen en daarvan de gemiddelde prestaties te berekenen. Inmiddels voldoet Nike aan de wet.

De zaak Bluetrace

Ook het volgen van mensen in en rond winkels via de wifi-signalen van hun mobiele apparaten — locatiegegevens — *zonder de winkelbezoeker of voorbijganger hierover te informeren*, is in strijd met de Wet bescherming persoonsgegevens, aldus concludeert de toezichthouder. Bluetrace levert technologie waarmee in en rondom winkels de wifi-signalen van mobiele apparaten worden opgevangen. Bovendien verzamelt, analyseert en bewaart Bluetrace meer gegevens dan noodzakelijk is, voor het in kaart brengen van bezoekersaantallen. Bluetrace heeft na het onderzoek aangegeven maatregelen te hebben getroffen, waaronder het *hashen* van gegevens en het verkorten van de bewaartermijn tot 48 uur. Echter, ondanks de getroffen maatregelen, handelt Bluetrace nog steeds in strijd met de wet. Op deze grond legde de toezichthouder het bedrijf een dwangsom op.[9]

De innovatieve entrepreneur komt niet onder *regulatory compliance* — het voldoen aan dwingendrechtelijke wet- en regelgeving — uit.

Werkprocessen

Dat digitalisering werk en werkprocessen verandert, blijkt onder meer uit werken op afstand. *Telecommuting*, ingegeven door problematisch woon-werkverkeer, maakte de afgelopen 40 jaar een forse ontwikkeling door. Het evolueerde gestaag dankzij telkens geavanceerdere digitale technologie tot zoiets als modern plaats- en tijdonafhankelijk werk. Ook het rechtskader ontwikkelde zich. Twee gebieden bepalen primair de kaders: arbeidsrecht en ICT-recht. *Het arbeidsrecht staat nieuwe manieren van werken nadrukkelijk niet in de weg* en is sinds 1 januari 2016 zelfs een geclausuleerd wettelijk recht geworden, dankzij de nieuwe Wet flexibel werken. De meest complexe uitdaging betreft de bescherming van de belangen van de werkgever via consolidatie en *fine-tuning* van het uiteenlopende recht, met als zwaartepunt het digitale recht, in de vorm van gedegen beleid per organisatie.[10]

[8] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nike-be%C3%ABindigt-overtredingen-hardloop-app

[9] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-wifi-tracker-bluetrace-last-onder-dwangsom-op

[10] Zie onder meer V.A. de Pous, *Het nieuwe werken in juridisch perspectief,* Amsterdam, 2014.

Nieuw digitaal HR-beleid

Bestaande personeelsgedragsregels voor computergebruik en Internet vragen in het licht van recente ontwikkelingen, zoals de onbepaalde derde werkplek, mobiel - en cloud computing, en *bring your own device*, dringend om een grondige reformatie. Digitalisering — zowel aanschaf en gebruik — ontsnapt tegenwoordig namelijk in toenemende mate aan de aandacht van de bestuurskamer, die daar toch voor verantwoordelijk is. Werknemers gebruiken mede eigen apparatuur, en vaak belangrijker, zelfgekozen en geïnstalleerde software en apps *ten dienste van hun arbeid*. Ook hiervoor blijft de werkgever verantwoordelijk en aansprakelijk.

Naast het risico op het gebruik van onveilige of illegale software, onttrekt de verwerking van de bedrijfsinformatie zich aan overzicht en controle van het bestuur van een organisatie.[11] Niemand weet waar welke — kopieën van bestanden van — bedrijfsdata zich bevindt, laat staan wie inzicht heeft of deze informatie (en de digitale technologie) in overeenstemming met wettelijke en contractuele voorschriften worden verwerkt.

Verdienmodellen

Sinds 2015 wil minister Kamp (Economische Zaken) samen met andere bewindslieden knelpunten in wet- en regelgeving voor 'ontwrichtende' technologiebedrijven vaststellen. De motivering luidt eenvoudig: de overheid staat vernieuwende ondernemers soms in de weg. Voorzichtigheid bij wetswijziging is echter geboden. Ten aanzien van de schaarse succesvolle en telkens aangehaalde exponenten van de *deeleconomie* — Airbnb en deels UBER[12] — wijzen we op de kennelijk belangrijke juridische waterscheiding tussen consument en degene die handelt in de uitoefening van een beroep of bedrijf. Kennelijk, omdat deze Chinese muur in veel rechtsgebieden is opgetrokken; ook door de Nederlandse wetgever.

Wetssystematische scheiding

Wetgevers brachten in de loop der jaren namelijk een wetsystematische scheiding aan tussen consumenten en hen die handelen uit hoofde van een beroep of bedrijf. Daarnaast normeert het mededingingsrecht eerlijke concurrentie in iedere sector; gereguleerd of niet. Met beide worstelt de deeleconomie fundamenteel. Wie zich sterk maakt voor deel-economische toepassingen, zal tegelijkertijd met verve moeten pleiten voor een nieuw en *muldisciplinair* rechtskader, dat nauwgezet aangeeft wat in nieuwe verhoudingen

[11] Verwerking (van persoonsgegevens) betreft volgens artikel 1, onder b Wet bescherming persoonsgegevens een ruim begrip: 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'.

[12] De politierechter deed vorig jaar uitspraak in acht zaken tegen chauffeurs, deels studenten, die taxidiensten hadden verricht met behulp van de app Uberpop. In alle procedures zijn voorwaardelijke geldboetes tussen de 1.500 en 3.000 euro opgelegd. OPENBAAR MINISTERIE V. ACHT TAXICHAUFFEURS, Rechtbank Rotterdam, 21 januari 2016.

geoorloofde mededinging is, zodat rechtszekerheid voor alle betrokkenen wordt geboden. Algemeen geldt dat *legal compliance* (in overeenstemming met wet, contract en beleidsregels handelen) eens te meer om zorgvuldigheid vraagt. Daarbij blijft analytisch vermogen onverkort vereist. Het intermediaire platform dan wel de vervoersdienst[13] UBER betreft namelijk geen exponent van delen; UberPop's vervoer met privéauto's wel, maar is in ieder geval op grond van het Nederlandse recht illegaal.

De gevolgen van digitale transformatie kunnen per bedrijfstak verschillen. Neem de muziekindustrie, die bijna het loodje legde door grootschalige online-piraterij. Is dat innovatief? Ontwrichtend? Beide vragen beantwoorden we bevestigend. Maar tegelijkertijd gaat het om onrechtmatig en wederrechtelijk handelen, dus strijdig met normen zowel uit het burgerlijk recht als het strafrecht. Die kant moeten we niet op. Kijkend naar fintech — ook een potentieel ontwrichtend commercieel domein — wijzen we op de bestaande, juridisch-geborgde financiële stabiliteit, welke cruciaal voor de samenleving is.

Elektronische identiteit en vertrouwensdiensten

Voor veilige en betrouwbare toegang tot digitale dienstverlening betreffen identificatie en *authenticatie* een basisvereiste. Ten aanzien van een digitaal werkende (semi)overheid werkt de regering aan de Wet Generieke Digitale Infrastructuur, die op 22 december 2016 in consultatie is gegaan.[14] Authenticatie — volgens het wetsontwerp: een 'elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon of rechtspersoon' — gebeurt door middel van erkende (i) publiek en (ii) privaat uitgegeven middelen. Het wetsvoorstel GDI sluit aan bij de Europese verordening elektronische identiteiten en vertrouwensdiensten, kortweg eIDAS genoemd.

eIDAS heeft per 1 juli 2016 de bestaande elektronische handtekeningenwetgeving, opgenomen in het BW, vervangen. Voor het grootste deel is eIDAS nu in werking. Let op: het gaat om een verordening, die op grond van het Europese recht een directe werking kent. Omzetting in nationaal recht is derhalve overbodig, maar om een uitvoeringswet kan lidstaat doorgaans niet heen. Op 6 december 2016 stemde de Tweede Kamer in met het wetsvoorstel uitvoering eIDAS.[15] Na goedkeuring door de Eerste Kamer gaat Agentschap Telecom toezicht houden op verleners van vertrouwensdiensten. Het wetsvoorstel regelt onder meer de benodigde bevoegdheden voor het *toezicht op verleners van vertrouwens-diensten*. Op dit moment ligt het toezicht op aanbieders van gekwalificeerde certificaten voor elektronische handtekeningen nog bij de Autoriteit Consument en Markt.

[13] Buitengemeen interessant: hierover wordt strijd gevoerd voor de rechter. De uitkomst is namelijk van belang voor de vraag welk rechtskader van toepassing is op het bedrijfsmodel.

[14] https://www.internetconsultatie.nl/wetgdi

[15] Voorstel van wet tot Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht, alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) (Kamerstuknummer 34 413).

Grensoverschrijdende transacties

De Europese Commissie wil nadrukkelijk stimuleren, dat nationale eID stelsels gebruikt kunnen worden voor grensoverschrijdende, veilige transacties door middel van wederzijdse erkenning. *De actuele juridische normering richt zich daarom op elektronische identificatie en zes elektronische vertrouwensdiensten*. De verordening normeert dus op tweeërlei wijze.

- Enerzijds gaat het om *elektronische identificatie.* Dat wil zeggen dat de regeling voorwaarden schept waaronder lidstaten elektronische identificatiemiddelen van natuurlijke en rechtspersonen erkennen, die onder een aangemeld elektronisch identificatiestelsel van een andere lidstaat vallen (indien een lidstaat haar nationale eID stelsel heeft aangemeld bij de Europese Commissie, moeten lidstaten elkaars stelsel accepteren).
- Anderzijds worden zes *elektronische vertrouwensdiensten* benoemd (i) handtekeningen, (ii) zegels, (iii) tijdstempels, (iv) documenten, (v) diensten voor elektronisch geregistreerde bezorging en (vi) certificatendiensten voor website-authenticatie. Allen krijgen een wettelijk kader (voor elektronische handtekeningen bestond dat dus al). Het betreft een gesloten lijst.

Nederlandse praktijk

In dit perspectief gaan de ontwikkelingen nu rap, maar wellicht beseft niet iedereen dit. Wij noteren opmerkelijke voorbeelden van eigen bodem. Wie bijvoorbeeld bij ziektekosten-verzekeraar Ohra wil inloggen, moet daarvoor tegenwoordig DigiD gebruiken; nota bene het identificatiemiddel van de overheid.[16] Een andere casus ziet toe op de Nederlandse banken, die samen met Betaalvereniging Nederland iDIN hebben ontwikkeld: een online identificatie- en inlogdienst. Met behulp hiervan kunnen particuliere rekeninghouders zich online identificeren en inloggen bij aangesloten organisaties — de zogenoemde acceptanten — met de inlogmiddelen van hun bank. De pilot startte op 8 maart 2016.[17]

Hierdoor verkrijgt de iDIN-acceptant — bedrijf of overheidsorganisatie — zekerheid over de identiteit van zijn online-klant, maar de acceptant heeft of krijgt nadrukkelijk geen toegang tot financiële gegevens van de klant bij zijn bank, zoals saldo- of transactiegegevens. Na het identificeren of inloggen wordt de verbinding tussen bank en acceptant weer verbroken. Vice versa kunnen de banken ook niet bij de gegevens over de klant bij een iDIN-acceptant, zoals de bezochte webpagina's en zijn bestellingen.

Het wetsontwerp Generieke Digitale Infrastructuur en de Europese verordening elektronische identiteiten en vertrouwensdiensten richten zich nadrukkelijk op het vergroten van het *vertrouwen in elektronische transacties*, door middel van een gemeenschappelijke basis — standaarden, acceptatie, beveiliging, meldplichten — zelfs voor wat betreft de Europese Unie, grensoverschrijdend.

[16] https://mijn.ohrazv.nl/

[17] https://www.betaalvereniging.nl/nieuws/pilot-idin/

Verwerking van persoonsgegevens

We hebben met betrekking tot de zaken Nike en Bluetrace gezien, dat het privacyrecht een ander belangrijk — en piketpaalstellend — rechtsdomein voor innovatie en digitalisering is. Bezien vanuit de positie van bedrijf of overheidsorganisatie maken persoonsgegevens in beginsel altijd deel uit van het cluster bedrijfsinformatie, naast bijvoorbeeld financiële data, marketingplannen en technische knowhow. Persoonsgegevens bestaan in hoofdzaak uit zowel klantgegevens in soorten en maten (van burger, consument of bijvoorbeeld patiënt), als gegevens van werknemers en freelancers. Sommige bedrijfstakken, zoals de reis- en hospitalitysector of de telecommunicatiesector, verwerken meer persoonsgegevens dan anderen, terwijl sommige sectoren bovendien tevens een bijzondere categorie persoonsgegevens verwerken, zoals iemands ras, godsdienst of gezondheid. Die worden '*gevoelige gegevens*' genoemd en zijn door de wetgever extra beschermd.

Aangescherpt regime

Ook bij de vernieuwing van het privacyrecht — net zo als bij het recht voor elektronische identiteit en vertrouwensdiensten — heeft de Europese Commissie voor het juridisch instrument verordening gekozen. Op 14 april 2016 stemde het Europees Parlement plenair in met de Algemene Verordening Gegevensbescherming, die per 25 mei 2018 de Wet bescherming persoonsgegevens vervangt. De AVG heeft enerzijds tot doel burgers meer controle over hun persoonsgegevens te geven. Anderzijds worden de verschillen in privacywetgeving tussen de 28 lidstaten van de Europese Unie door middel van de *rechtstreekse werking* van de verordening verkleind. De verplichtingen van de verantwoordelijken nemen toe.

5500 datalekken gemeld

Vooruitlopend op de AVG heeft Nederland autonoom de Wet meldplicht datalekken geïntroduceerd, welke op 1 januari 2016 in werking trad.[18] Dat zal vrijwel niemand zijn ontgaan. Organisaties die een ernstig datalek hebben, moeten dit sindsdien melden bij de Autoriteit Persoonsgegevens en soms ook aan de mensen van wie de gelekte gegevens zijn; in wettelijk jargon de 'betrokkenen'. Tot 15 december 2016 heeft deze toezichthouder bijna 5500 meldingen ontvangen van datalekken. Inmiddels zijn tientallen onderzoeken naar aanleiding van datalekmeldingen opgestart.[19]

Een wettelijke meldplicht voor een digitaal incident, inclusief voor een lek van persoonsgegevens, *kan* te maken hebben met criminaliteit. Dat hoeft echter nadrukkelijk niet het geval te zijn. Een officier van justitie zet een PC bij het oud vuil, er gaat iets mis met een *software patch*, een gemeenteambtenaar stuurt persoonsgegevens naar een verkeerd mailadres, en wat dies meer zij. Vaak ontbreekt opzet en is er geen sprake van cybercrime. Dat bevestigt de toezichthouder nadrukkelijk. Er zijn veel datalekken waarbij gegevens onbedoeld bij iemand anders terecht komen. 'Bijvoorbeeld door een verkeerd bezorgde brief, een e-mail aan de verkeerde ontvanger of als een klant in een klantportaal de gegevens van iemand anders ziet. Ook komt het vaak voor dat bijvoorbeeld een USB-stick met persoonsgegevens kwijtraakt of een laptop wordt gestolen.'

[18] Wet van 4 juni 2015. Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid.

[19] https://autoriteitpersoonsgegevens.nl/nl/nieuws/1-jaar-meldplicht-datalekken

Digitale beveiliging en meldplichten

Netwerk- en informatiebeveiliging betreft op grond van het in Nederland geldende recht — autonoom Nederlands recht en Europees recht — een *geconsolideerde wettelijke verplichting*. Dat wil zeggen dat uiteenlopende wet- en regelgeving voorschriften stellen aan de beveiliging van digitale technologie en gegevens tegen verlies en diefstal of onrechtmatige verwerking. Het gaat dus om meer wetgeving dan de Wet bescherming persoonsgegevens alleen. Vaak hanteren zowel leveranciers als gebruikersorganisaties eigen omschrijvingen van netwerk- en informatiebeveiliging; juristen kijken naar de wettelijke insteek. Om een formeel-juridische definitie van digitale beveiliging aan te halen:

'het vermogen van een netwerk- en informatiesysteem om met een bepaald niveau van betrouwbaarheid bestand te zijn tegen accidentele gebeurtenissen of opzettelijke handelingen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen of verzonden gegevens of de daaraan gerelateerde diensten die via dat netwerk- en informatiesysteem worden aangeboden of toegankelijk zijn, in gevaar brengen'.[20]

Digitale incidenten

De wettelijke beveiligingstrend zet zich gestaag door, inclusief eveneens wettelijke meldplichten voor uiteenlopende ICT-gerelateerde incidenten. Zo gaf het Europese Parlement op 6 juli 2016 groen licht voor de Richtlijn netwerk- en informatiebeveiliging.[21] Op grond hiervan worden 'Digital Service Providers' (DSP's) — aanbieders van zogenoemde 'essentiële diensten' — verplicht om inbreuken in hun informatiesystemen te melden. *Deze meldplicht gaat verder dan de geldende of aankomende autonome Nederlandse wetgeving*.[22]

Digitale incidenten tonen zich verschillend, bijvoorbeeld (een vermoeden van) een lek van persoonsgegevens, een veiligheidsinbreuk of integriteitsverlies. Sommigen van de informatievoorschriften zijn smal (sectoraal); anderen breed (voor alle organisaties). Daarnaast kenden we al meldplichten voor andersoortige voorvallen, zoals vastgelegd in de Wet financieel toezicht: incidenten die betrekking hebben op *integere bedrijfsvoering*.[23] Doorredenerend komen we overigens hier — mede — uit op computercriminaliteit in soorten en maten.

---

[20] Artikel 3, lid 2 van de Europese Richtlijn netwerk- en informatiebeveiliging.

[21] Voorstel voor een Richtlijn van het Europees parlement en de Raad inhoudende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM (2013) 48 final, 2013/0027 (COD), 7 februari 2013 (Europese Richtlijn netwerk- en informatiebeveiliging). De richtlijn trad op 1 augustus 2016 in werking. Lidstaten hebben vervolgens 21 maanden om de nieuwe regels van de richtlijn om te zetten in eigen wetgeving, dus voor 1 mei 2018.

[22] Digital Service Providers zijn volgens de richtlijn 'iedere rechtspersoon die een digitale dienst levert, zoals online-marktplaatsen, zoekmachines en cloud computing diensten.' Let op de uitzonderingen. Zo sluit de richtlijn hard- en softwarebedrijven, aanbieders van vertrouwensdiensten en DSP's met minder dan 50 medewerkers en minder dan 10 miljoen euro omzet expliciet uit.

[23] Artikelen 3:10 lid 3 en 4:11 lid 4 Wet financieel toezicht. Toezichthouders zijn De Nederlandse Bank en de Autoriteit Financiële Markten. Soms moet er ook aan cliënten worden gemeld, die vervolgens recht hebben op een schadeloosstelling.

Melden of juist niet?

Er heerst verwarring. Het FD kopte recent 'Niet melden van cybercrime is vaak verstandiger' naar aanleiding van een interview met een advocaat, oud-officier van justitie.[24] De discussie dateert uit de jaren zestig van de vorige eeuw, toen de eerste zaken van computermisbruik aan het licht kwamen. Omdat vriend en vijand er destijds van uitging dat deze incidenten — veelal vermogensdelict of sabotage — doorgaans niet tot aangifte leidden wegens angst voor reputatieschade, werd de omvang van computercriminaliteit steevast vergeleken met het topje van een ijsberg. *Dark numbers.* Die situatie is vandaag onveranderd, maar de schaal nam wel exponentieel toe.

Onzuivere discussie

Wie adviseert geen digitale criminaliteit te melden, heeft deze vrijheid. *Het Nederlandse recht kent immers geen algemeen voorschrift om cybercrime — aan wie dan ook — te melden*. Bovendien: bedrijven mogen risico's nemen (maar openbaar bestuur en ambtenaar nadrukkelijk niet). De discussie moeten we zuiver voeren. Zoals gezegd, is het huidige digitale meldplichtspectrum breed en breidt bovendien telkens uit. Deze 'juridische lappendeken' brengt een veel groter — geconsolideerd — risico voor gedigitaliseerde organisaties met zich mee, dan het gedoe omtrent de nieuwe Wet meldplicht datalekken, waar kennelijk een groot deel van de samenleving aan moet wennen.[25]

Serieus risico

De diverse meldingen (wanneer moet wat door wie worden gemeld) verschillen onderling inhoudelijk. Dat geldt ook voor de te volgen procedure (aan welke toezichthouder en/of andere partij moet er op welke wijze en binnen welke termijn worden gemeld). Hierdoor trekken verwarring en aansprakelijkheid waarschijnlijk gelijk op met de stijging van deze categorie juridische verplichtingen, terwijl de administratiefrechtelijke boetes ook nog eens recent fors verhoogd zijn (bijvoorbeeld EURO 820.000 per overtreding of 10% van de omzet). Let op. Er kunnen zelfs *digitaal-gerelateerde meldplichten uit overeenkomst* (onbenoemd en benoemd) ontstaan tegenover een contractspartij, alsook uit *onrechtmatige daad*, jegens een individu of organisatie, die schade leidt door een dergelijk incident. Zo nieuw zijn meldplichten dus niet.

Bij de meeste meldplichten gaat het *om het beperken van schade* en om het stimuleren van vertrouwen in een bepaalde sector of, breder, de samenleving. Voor de Wet meldplicht datalekken is dat niet anders.[26] De informatiesamenleving heeft dringend behoefte aan meer vertrouwen van de burger en meldplichten ondersteunen vertrouwen.

[24] Voorpagina 24 oktober 2016.

[25] *Data breach notification laws* zijn geen novum. Veel Amerikaanse staten begonnen met deze wetgeving aan het begin van deze eeuw; California — met Silicon Valley — was nota bene de eerste in 2003. Voor telecombedrijven en ISP's in de Europese Unie geldt een dergelijke verplichting sinds 25 mei 2011.

[26] Het staat buiten kijf dat iedere klant graag zo snel mogelijk wil weten of zijn account is gehackt. De klant kan dan zelf bepalen wat de vervolgstappen zijn om zijn schade te beperken, en meer. Daarnaast kun je je afvragen of een aandeelhouder tevreden is met het onder de pet houden van een grootschalig ICT-gerelateerd incident.

Conclusies

Digitalisering behoort rechtmatig plaats te vinden en dat geldt onverkort wanneer een transformatie digitaal tot bedrijfseconomische of maatschappelijke ontwrichting leidt. Minister Kamp (Economische Zaken) vindt dat we commerciële verandering niet moeten tegenhouden. Samen met de bewindslieden van Binnenlandse Zaken en Veiligheid en Justitie verkent hij op welke wijze wetgeving vaker op hoofdlijnen, toekomstbestendig of technologieneutraal opgesteld kan worden. 'Dat stelt bedrijven in staat om nieuwe innovaties sneller te introduceren, omdat er mogelijk belemmerende detailvoorwaarden minder vaak worden vastgelegd.'[27]

Ieder geval voor wat betreft de deeleconomie — *collaborative consumption* of *peer economy* — is dat makkelijker gezegd dan gedaan, omdat deze vorm van bedrijvigheid de *inhoudelijke* wetssystematiek raakt. Materiële normen maken immers bewust scherp onderscheid in rechtsposities, zoals tussen degene die handelt in de uitoefening van een beroep of bedrijf en de consument. Daarnaast kennen we gereguleerde sectoren, waarvoor mede bijzondere regels gelden; van telecommunicatie tot personenvervoer, van financiële dienstverlening tot *healthcare*.

Ondertussen dijt het digital recht telkens fors uit. Toch behoort dit rechtsgebied tenminste op hoofdlijnen thuis in de bestuurskamer van bedrijf en overheidsorganisatie, omdat digitaal recht het fundament vormt voor — ondernemen en openbaar besturen in — de informatiesamenleving en dat geldt zo mogelijk in het bijzonder voor ICT-bedrijven, die vanoudsher zowel aan inkoop- als verkoopkant bits en bytes in hun DNA hebben. Wie bij de ontwikkeling van een product of dienst onvoldoende oog heeft voor het dwingende rechtskader van digitalisering, kan van rechter of toezichthouder lik op stuk krijgen.

Voldoen aan wet- en regelgeving is voor een organisatie echter geen doel als zodanig, zorgvuldig omgaan met bedrijfsinformatie betreft minimaal een *strategische randvoorwaarde*. Dit uitgangspunt komt goed naar voren bij het privacyrecht. Bij de verwerking van persoonsgegevens staat immers *de positie van de betrokkene* — degene wiens gegevens worden verwerkt — *centraal*. Weeg dus niet alleen de administratieve lastendruk, maar besef de ratio van een regeling.

Vaststaat bovendien dat trendy arbeidsmodernismen, zoals *bring-your-own-device* en nieuwe manieren van plaats- en tijdonafhankelijk werk, de juridische risico's van digitale organisaties verhogen, inclusief met betrekking tot het verzuim van digitale meldplichten.

Pak digitale techniek en digitale bedrijfsinformatie, inclusief archivering en e-depots, juridisch-beleidsmatig *integraal* aan.

[27] https://www.rijksoverheid.nl/actueel/nieuws/2015/07/20/kamp-nederland-als-eerste-laten-profiteren-van-vernieuwing

COLOFON

Juridische trends in digitale transformatie is geschreven door Mr. V.A. de Pous, zelfstandig bedrijfsjurist en industrieanalist te Amsterdam. De auteur houdt zich sinds 1983 bezig met de rechtsaspecten van digitale technologie, elektronische gegevensverwerking en de informatiemaatschappij en geeft sinds 1987 de nieuwsbrief NEWSWARE uit. Eindredactie: M.L. Baan.

SELECTIEVE BIBLIOGRAFIE

Computerrecht, Amsterdam, 1982

Het recht van overheidsautomatisering, Stichting het Expertise Centrum, Den Haag, 1995

Het recht op stroomlijning basisregistraties; Juridisch kader authentieke registraties, ICTU, Den Haag, 2002

Open source software en politiek / Open Source Software and Politics / オープンソースソフトウエアと政策 / 开源软件及政策, Amsterdam, 2004

Recht op ICT-interoperabiliteit, GBO.Overheid, Den Haag, 2008

Data Storage Recht; Wat managers en ICT-professionals behoren te weten, Amsterdam, derde druk, 2009

In and out-of-office working; Juridische aspecten van het nieuwe werken voor werkgevers, Amsterdam, 2009

Zakendoen met de overheid; Public procurement voor ICT-leveranciers, Amsterdam, 2010

Softwarekwaliteit en garantierechten, Amsterdam, 2010

Open Source Computing and Public Sector Policy, Amsterdam, 2012 (updated version)

Cloud Computing and Public Sector Policy, Amsterdam, 2013

Efficiënt automatiseren; Praktijkvisies op Cloud Computing (2), Baarn, 2014

Naar intelligent recht voor smart cities, Amsterdam, 2014

Cloud computing en het Amerikaanse overheidsbeleid (voor Forum en College Standaardisatie), Amsterdam, 2015

Cloud computing in juridisch perspectief 2016, Amsterdam, 2016

Julianapark, Anton Constandsestraat 16, Postbus 51005, 1007 EA Amsterdam
Telefoon: 020-665.57.38, E-mail: depous@protonmail.com
Fonds: http://technologierecht.blogspot.com/
LinkedIn : https://www.linkedin.com/in/victordepous

Leitmotiv
Addressing the legal aspects of digital technology strategically creates economic value, reduces risks and optimizes assets.

History
During its first 50 years computer law referred to a loose collection of diverse legal aspects of electronic processing and communication of data.

Advancement
A more advanced and structured approach to computer law in the 21st century focuses on legal frameworks for the demand-driven availability of robust, secure and interoperable digital products and services.

Information society
Computer law today must provide solid, well-balanced legal constructions for living, working, and doing business in a sustainable information society, fitting to its people and national identity.