Public Briefing / januari 2015

Een juridische vooruitblik: vertrouwen in de informatiemaatschappij centraal

Mr. V.A. de Pous[1]

Cloud computing — inmiddels de hype voorbij — vormt de drijvende kracht achter veel bestaande en ontluikende elektronische toepassingen. Van big data tot *the Internet of Things*. Sterker nog, in toenemende mate zijn clouddiensten synoniem geworden voor ICT. Vertrouwen in de informatiemaatschappij staat vandaag echter onder druk. In door cloud computing gedreven ontwikkelingen domineert de discussie over informatiebeveiliging en de bescherming van de persoonlijke levenssfeer; *ook in het voortsnellende recht*.

Wetgeving, wetgeving en nog eens wetgeving

De tijdgeest toont zich buitengemeen dynamisch. Alles in verandering; alles op de schop. Althans zo lijkt het; *ook* in het rechtsdomein. Veel legislatieve en andere juridische ontwikkelingen raken het door mij benoemde containerbegrip 'vertrouwen in de informatiemaatschappij', dat als cruciale voorwaarde voor duurzaam succes fungeert. Belangrijke aspecten of verschijningsvormen daarvan betreffen de beveiliging van (i) de elektronische gegevensverwerking algemeen en (ii) onze persoonlijke levenssfeer in het bijzonder. Beiden zijn doorgaans onvermijdelijk met cloud computing als de exclusieve hofleverancier voor digitale technologie en informatievoorziening verbonden. Een greep uit de wettelijke blauwdrukken.

[1] Victor de Pous is bestuurslid van de Stichting EuroCloud Nederland en zelfstandig bedrijfsjurist sinds 1983.

Algemene Verordening Gegevensbescherming
Europa gaat dit jaar eindelijk de in januari 2012 geïntroduceerde *Algemene Verordening Gegevensbescherming* vaststellen, waardoor onze Wet bescherming persoonsgegevens ingetrokken wordt en er in de interne markt een uniform en aangescherpt regime komt voor de verwerking van persoonsgegevens. Met rechtstreekse werking en dwingend van karakter. Geen nationale afwijking mogelijk, inclusief de beoogde aangescherpte en nieuwe privacyrechten, strikte beveiligingsvoorschriften, nieuwe meldplichten en zware sancties bij overtreding. Zo wordt het niet melden van een verwerking van persoonsgegevens gezien als een *economisch delict* en dus strafbaar (op grond van het Wetboek van Strafrecht).

Verordening Elektronische Identiteiten en Vertrouwensdiensten
Europa werkte de afgelopen jaren eveneens aan de *Verordening Elektronische Identiteiten en Vertrouwensdiensten* in de interne markt. De Europese Raad van Ministers heeft deze eIDAS Verordening vorig jaar zomer goedgekeurd. De nieuwe regeling vervangt de bestaande wetgeving die alleen betrekking heeft op de elektronische handtekening. Brussel wil stimuleren dat nationale eID stelsels gebruikt kunnen worden voor *grensoverschrijdendeveilige* transacties door wederzijdse erkenning. De juridische normering richt zich op *elektronische identificatie en elektronische vertrouwensdiensten.*

Bij identificatie gaat het om voorwaarden waaronder lidstaten elektronische identificatie-middelen van natuurlijke en rechtspersonen erkennen die onder een aangemeld elektronisch identificatiestelsel van een andere lidstaat vallen. Ten aanzien van *elektronische vertrouwensdiensten* worden er in totaal zes 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 bestaat dat dus al). Het betreft een gesloten lijst.

Richtlijn voor netwerk- en informatiebeveiliging
In het domein *cybersecurity* ligt er sinds februari 2013 een communautaire richtlijn ter tafel, de Richtlijn voor netwerk- en informatiebeveiliging. Dit ontwerp bepaalt onder meer dat exploitanten van essentiële infrastructuur in een aantal sectoren (financiële dienstverlening, vervoer, energie, gezondheidszorg), aanbieders van diensten van de informatiemaatschappij (met name appstores, platforms voor elektronische handel, betalingsdiensten via Internet, cloud computing, zoekmachines en sociale netwerken) en overheden (i) *risicobeheers-regelingen* moeten invoeren en tevens (ii) ernstige incidenten met betrekking tot hun kerndiensten *moeten melden*. Over de reikwijdte bestaat echter nog geen consensus. Wanneer de richtlijn in de eerste helft van 2015 wordt vastgesteld, treedt hij voor het einde van 2016 in werking.

Nederland ICT-legislatief

Met al het wetgevingsgeweld uit de Europese Unie zou je bijna vergeten dat Nederland een soevereine staat is met een in de Grondwet verankerde bevoegdheid tot maken van autonome wetgeving. Dat gebeurt natuurlijk ook. Zelfs de doorgaans kritische Raad van State wees onlangs op een belangrijke rechtsregel. Het enkele feit dat de Europese rechter een Europese wet — zoals de van begin af aan omstreden Richtlijn dataretentie inzake verkeergegevens telecommunicatie uit 2006 — onrechtmatig verklaart, wil niet zeggen dat de hierop gebaseerde Nederlandse wetgeving eveneens onrechtmatig is.

Wet bewaarplicht telecommunicatiegegevens
De regering gaat de Wet bewaarplicht telecommunicatiegegevens aanpassen naar aanleiding van het Digital Rights Ireland en Seitlinger arrest. Zoals bekend, verklaarde het Hof van Justitie van de Europese Unie op 8 april 2014 de Europese Richtlijn gegevensbewaring met terugwerkende kracht ongeldig wegens schending van grondrechten. Onze wet betreft de uitwerking van deze richtlijn. Het kabinet verzwaart onder meer de eisen voor toegang tot de telecommunicatie-gegevens, zo blijkt uit de verlate reactie uit Den Haag.'De Nederlandse wetgever heeft een algemene bevoegdheid om regels te stellen. De Nederlandse wetgeving bevat reeds waarborgen die verder gaan dan die van de richtlijn dataretentie, zoals de regels in het Wetboek van Strafvordering over de toegang tot de bewaarde gegevens', aldus het kabinet.

Zowel Telecommunicatie-wet als Wetboek van Strafvordering worden gewijzigd. Zo kan straks de vordering van de officier van justitie tot het verstrekken van telecommunicatiegegevens slechts worden gegeven *na een voorafgaande machtiging door de rechter-commissaris*. Verder wordt de toegang tot de gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven gedifferentieerd *aan de hand van de ernst van het misdrijf*.

Een telkens maatschappijbreder-wordende coalitie is faliekant tegen en heeft de Staat gedaagd. Een uitspraak kunnen we dit jaar tegemoet zien. Ook het College bescherming persoonsgegevens blijft forse kritiek houden op de wettelijke datarentievoorschriften. Al in 2002 stelde het CBP dat een systematische opslag van deze gegevens voor een periode van een jaar of meer onevenredig is en in geen geval toelaatbaar.

Wet op de inlichtingen- en veiligheidsdiensten
Verder wordt de Wet op de inlichtingen- en veiligheidsdiensten aangepast. De ongeveer vijftien jaar oude wet maakt onderscheid tussen de ether en kabel, terwijl 90% van de telecommunicatie tegenwoordig via de kabel verloopt. In de

gewijzigde wet krijgen de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst de bevoegdheid om ook via de kabel tijdig terroristische dreiging te kunnen onderkennen, spionage tegen te gaan, bescherming te bieden tegen digitale aanvallen, de Nederlandse veiligheids-belangen te dienen en militaire missies te ondersteunen.

Uit oogpunt van terrorismebestrijding wil het kabinet de diensten onder voorwaarden toestaan om op de kabel *ruwe* telecommunicatiegegevens te onderscheppen. Door de waarborgen in elke fase van het onderscheppen en verwerken van gegevens, kan de overheid niet in willekeurige e-mailconversaties van burgers meekijken of telefoongesprekken meeluisteren.

Wet meldplicht datalekken en uitbreiding boetebevoegdheid
Terwijl de Wet bescherming persoonsgegevens sowieso wordt ingetrokken — en vervangen door de Europese Algemene Verordening Gegevensbescherming — blijft het kabinet vasthouden aan het voornemen onze privacywet nog voor de inwerkingtreding van de AVG te wijzigen met het oog op (i) de invoering van een meldplicht bij doorbreking van maatregelen voor de beveiliging van persoonsgegevens en (ii) de uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen.

Eerder uitte de Raad van State forse kritiek op de meldplicht, zoals geregeld in het eerste wetsvoorstel — veel te vaag — nu tekent het CBP onder meer bezwaar aan tegen wijzigingen om administratiefrechtelijke boetes op te leggen. In het laatste voorstel stijgt de maximale sanctie van EURO 4.500 tot weliswaar EURO 810.000, maar volgens voorzitter Kohnstamm werpt het wetsvoorstel teveel drempels op voordat überhaupt een serieuze boete gegeven kan worden. ‘We moeten drie of vier gele kaarten geven, voordat iemand het veld uitgestuurd kan worden. Bescherming persoonsgegevens is het in de ogen van staatssecretaris Teeven kennelijk niet waard om de toezichthouder een serieuze boetebevoegdheid te geven.’

Los van de inhoudelijke bezwaren, blijft het opmerkelijk dat het kabinet slechts voor korte duur ingrijpende wetswijzigingen wil doorvoeren. Met de aanstaande inwerkingtreding van de AVG — nu in 2016 voorzien — komt er ook een meldplicht bij datalekken en wordt de maximale boete die een toezichthouder kan opleggen EURO 100.000.000 of, indien hoger, 5% van de wereldwijde omzet van een onderneming.

Tot slot

In samenhang met al het wetgevingsgeweld constateren we tenminste twee majeure problemen. Allereerst ontbreekt bij wetgever, politiek en openbaar bestuur een algemeen vergezicht voor onze *informatie*samenleving, gefundeerd op stevige uitgangspunten en kernwaarden. Vrijheid en democratie zijn de kernwaarden van Nederland, aldus het kabinet. Laten we beginnen deze aan te vullen met het eveneens onvoorwaardelijke pendant 'rechtstaat' en bovendien in het overheidsbeleid de mens centraal zetten; ook c.q. juist bij elektronische gegevensverwerking.

Daarnaast doen de aanzienlijke hoeveelheid en snel in omvang toenemende, uiteenlopende *speciale* wetgeving (geheel nieuw of telkens wijzigend) en allerhande andere juridische veranderingen — die zich bovendien allemaal in hoog tempo en parallel voltrekken — voorspelbaar de alarmbellen rinkelen. Wie durft er nog op naleving te rekenen, terwijl compliance in de informatie-maatschappij, mede gelet op schaalgrootte, sowieso onder druk staat?