PUBLIC BRIEFING / JANUARI 2016

Een juridische vooruitblik: ICT-wetgeving ingeklemd tussen handelsbelang en veiligheid

Cloud computing verovert de wereld met een voortvarendheid waar eerdere modellen voor elektronische technologie en gegevensverwerking met jaloezie naar kijken. Ook juridisch bezien zet spoedeisendheid grotendeels de toon. Nationale wetgevers produceren in hoog tempo een bonte verzameling autonome ICT-gerelateerde regels die cloud computing vaak in het hart raken. De informatiemaatschappij bevindt zich daardoor juridisch ingeklemd tussen handelsbelang en nationale veiligheid. Ondertussen ploegt de Europese Unie noestig verder voor het realiseren van een *digital single market*, nieuwe wetgeving inzake privacy en netwerk- en informatiebeveiliging incluis.

Mr. V.A. de Pous[1]

Nationale ICT-wetgeving: een onvermijdelijk gegeven

Soevereine staten normeren *hun* informatiemaatschappij nadrukkelijk op basis van autonome wetgeving. De voorbeelden zijn legio. Zo verplicht Russisch recht tot dataopslag op Russisch grondgebied, overweegt het Verenigd Koninkrijk evenals bijvoorbeeld Frankrijk om encryptie bij wet te verbieden, terwijl de Duitse rechter Google's Gmail heeft aangemerkt als telecommunicatiedienst, waardoor sommige clouddiensten strikter worden genormeerd. Daarnaast zijn telecommunicatiebedrijven en Internet-aanbieders verplicht 'technische hulp' te bieden aan Chinese veiligheidsafdelingen om terroristische activiteiten te voorkomen, en wenst onze wetgever *op Nederland gerichte* online-kansspelen geclausuleerd mogelijk te maken. Eerder maakte Frankrijk van plannen om het TOR-netwerk te verbieden en het gebruik van openbare wifi-netwerken tijdens een noodtoestand te blokkeren. Die zijn inmiddels weer ingetrokken.

Van de autonome wetgevingsbevoegdheid en de keuze voor geheel nieuwe, afwijkende nationale ICT-wetgeving, getuigt eveneens het Nederlandse ontwerp Wet computer-criminaliteit III, eind december ingediend bij de Tweede Kamer,

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

dat politie en justitie de formele bevoegdheid geeft heimelijk 'terug te hacken'; zelfs grensoverschrijdend. Een uniek opsporingsmiddel. Nog een voorbeeld. De Verenigde Staten zet legislatief in op het delen van informatie over netwerkbeveiliging. Wie als bedrijf gegevens ter zake verstrekt aan het Department of Homeland Security heeft recht op juridische bescherming (maar moet overigens onder voorwaarden wel toegang tot klantgegevens verstrekken). En last but not least, iedere eigenaar van een drone in de VS moet tegenwoordig zijn onbemand luchtvaartuig formeel bij de Federal Aviation Administration registeren en deze markeren.

Balkanisatie

Sommigen, vooral grote ondernemingen, vrezen deze ontwikkeling: 'the Balkanization IT'. Dat betreft bij nader inzien minder ICT als zodanig, maar meer afzonderlijke digitale *markten,* dus gebieden met eigen spelregels. *Juridische* Balkanisatie kunnen we echter niet nieuw noemen. Sterker nog: zij heeft zo ongeveer vanaf *day one* bestaan. Recht wordt immers van oudsher nadrukkelijk geografisch bepaald. Dat uitgangspunt geldt onverkort ten aanzien van de juridische normering van de commerciële informatietechniek, die na de tweede wereldoorlog opkwam.

De actuele toename en diversiteit van nationale ICT wet- en regelgeving onderscheidt zich wel van vroeger. We zien veel nieuwe, bijzondere regels voor uiteenlopende digitale onderwerpen, die doorgaans snel tot stand komen. Uitzomend blijkt dat het om twee categorieën wet- en regelgeving gaat: gericht op handelsbelang of nationale veiligheid. Aanbieders van producten en diensten in het digitale domein worden hierdoor niet zelden frontaal geraakt. Aanpassen en *regulatory compliant* zijn, of land dan wel regio verlaten, luidt het devies. Veel smaken zijn er niet.

Worldwide public cloud

Microsoft zegt in ieder geval te hebben afscheid genomen van de wereldwijde *public cloud* door middel van haar recente besluit om persoonsgegevens van Europese burgers in Duitsland gevestigde datacenters van T-Systems te verwerken. Langs deze weg worden de persoonsgegevens en andere informatie van haar klanten buiten de reikwijdte van de Patriot Act en verwante Amerikaanse wetgeving geplaatst. Commentatoren kijken hier op allerlei manieren naar, maar *im Grunde genommen* gaat het toch vooral om pragmatisme. Microsoft doet wat haar Europese klanten graag willen (en houdt bedrijfsinformatie en persoonsgegevens in beginsel uit Amerikaanse overheidshanden). Daardoor is ze tevens *regulatory compliant*. Tegelijkertijd kun je je afvragen of het concept van een wereldwijde public cloud überhaupt juridisch realiseerbaar is. En vervolgens welke internationale afspraken hierbij

passen, zonder dat soevereine staten de zeggenschap over hun nationale veiligheidszaken (en handelsbelangen) verliezen.

Safe Harbour 2 niet op tijd voor Amerikaanse MKB-markt?

In antwoord op Kamervragen schreef minister Van der Steur (Veiligheid en Justitie) op 30 november 2015 dat hij niet verwacht dat de onderhandelingen over een nieuw Safe Harbour-verdrag, goed beschouwd een Europese beschikking, over de doorgifte van persoonsgegevens van Europese burgers naar de Verenigde Staten, op korte termijn zullen worden afgerond. Niet alleen werd de oude beschikking uit 2000 door het Gerechtshof van de Europese Unie op 6 oktober 2015 ongeldig verklaard — de Amerikaanse inlichtingendiensten verzamelen grootschalig persoonsgegevens van Europese burgers, terwijl aanspraak op effectieve gegevensbescherming ontbreekt — ook werkt de Europese Unie zoals bekend aan nieuwe privacywetgeving, die eveneens herziening van Safe Harbour vereist.

Deadline

Afronding en inwerkingtreding staan echter onder tijdsdruk omdat de in de Artikel 29 werkgroep verzamelde Europese privacytoezichthouders, de deadline op eind januari 2016 hebben gesteld. Bij gebreke aan een nieuw verdrag, mogen vanaf februari persoons-gegevens niet langer aan de Verenigde Staten worden doorgegeven, omdat het land geen passend beschermingsniveau voor Europeanen biedt. Let op: buiten deze omstandigheid is doorgifte toch toegestaan, echter uitsluitend op basis van een wettelijke uitzondering of met vergunning van de Minister van Justitie, na advies van de toezichthouder af te geven.

Standard Contract Clauses

Uitzonderingen bevestigen dus de regel. Wanneer het *binnen een multinational* om doorgifte naar een land zonder passend beschermingsniveau gaat, kunnen *interne* gedragscodes in de vorm van Binding Corporate Rules uitkomst bieden. In andere gevallen bestaat de mogelijkheid voor, in dit geval, *Amerikaanse* bedrijven, waaronder cloudleveranciers, door de Europese Unie opgestelde Standard Contract Clauses op te nemen in overeenkomsten met hun klanten (extern dus). Bij Safe Harbour waren grofweg 4000 bedrijven aangesloten. Het leeuwendeel daarvan betreft kleine(re) ondernemingen. Vooral deze groep zal naar verwachting snel moeten handelen, hetgeen mogelijk aanzienlijke kosten tot gevolg heeft. Gebruikers(organisaties) doen er goed aan om te vragen of de modelcontracten van toepassing zijn op hun rechtsverhouding.

Verdeelde meningen

Maar het kan ook zijn dat een strikte Duitse privacytoezichthouder roet in het eten gooit. Weliswaar vormen de Standard Contract Clauses een rechtsgeldige uitzonderingsregel; het Unabhängiges Landeszentrum für Datenschutz van Schleswig-Holstein beschouwt ze desalniettemin illegaal. Wie zonder wettelijke basis persoonsgegevens van Europeanen op servers in de VS opslaat, kan beboet worden met 300.000 euro, aldus deze toezichthouder. Dan kunnen de overeenkomsten met Amerikaanse cloudleveranciers beter beëindigd worden. Vrijwel zeker zullen de samenwerkende Europese privacytoezichthouders, verenigd in de inmiddels notoire Artikel 29 werkgroep, met een eensluidend standpunt komen. Dat betekent dat óf deze toezichthouder uit de Bondsrepubliek gelijk krijgt en het huidige systeem van wettelijke uitzonderingen deels op de schop gaat; óf dat, bij een andersluidend standpunt, Schleswig-Holstein zal moeten inbinden. Op 1 februari weten we meer.

Europese wetgeving

Op de valreep — 15 december — hebben Europees Parlement, de Europese Commissie en de lidstaten eindelijk een *voorlopige* overeenstemming bereikt over de Algemene Verordening Gegevensbescherming (AVG). Het voltallige parlement stemt er begin dit jaar over, dan wordt de tekst definitief vastgesteld en treedt de regeling twee jaar later in werking. In het eerste kwartaal van 2018 krijgt de Europese Unie voor het eerst een daadwerkelijk gelijk privacyspeelveld.

Zoals bekend, gaat het om een grondige herziening en actualisering, die bestaande privacyrechten aanscherpt, nieuwe toevoegt en tevens administratieve lasten wil verlichten. We zien onder meer regels over het inzage-, correctie en verwijderingsrecht van individuen (burgers, consumenten, patiënten, werknemers, en meer), alsook de verplichte aanstelling van een *privacy officer*, zij het onder voorwaarden. Verder bevat de verordening een meldplicht voor datalekken en voor het bedrijfsleven kan een toezichthouder een geldboete opleggen tot maximaal 4 procent van de jaaromzet.

Cybersecurity

Na ruim twee jaar onderhandelen lijkt een doorbraak te zijn bereikt over het ontwerp van een Richtlijn voor netwerk- en informatiebeveiliging (NIB). Op 7 december bereikten de Europese Commissie en de verantwoordelijke commissie van het Europees Parlement namelijk consensus. Hierna volgt parlementaire stemming (EP-Commissie Interne markt en consumentenbescherming en het Comité van Permanente Vertegenwoordigers) en als laatste de behandeling in de Telecomraad, de verzamelde telecomministers.

Het oorspronkelijke ontwerp bepaalt onder meer dat exploitanten van essentiële infrastructuur in een aantal sectoren (financiële dienstverlening, vervoer, energie, gezondheidszorg), aanbieders van diensten van de informatiemaatschappij (inclusief cloudleveranciers) en overheden *risicobeheersregelingen* moeten invoeren *en* ernstige incidenten met betrekking tot hun kerndiensten *moeten melden*. Vast staat dat het niveau van de beveiligingsvoorschriften is gekoppeld aan de maatschappelijke relevantie van een bedrijfstak. De jongste versie van de NIB-richtlijn is nog niet openbaar, maar naar verwachting wordt de tekst snel definitief gemaakt.

Tot slot

Stimulering van de eigen — digitale — economie enerzijds en nationale veiligheid anderzijds in de vorm van verregaande bevoegdheden voor overheidsdiensten inzake toegang tot informatie. Dat zien we duidelijk terug in wet- en regelgeving voor de informatiemaatschappij: *allerhande autonome regels en voorschriften, verschillend per soevereine staat*. De vraag is of dat anders kan.

Voor het internationaal luchtverkeer mogen regels omtrent aansprakelijkheid bij verdrag zijn vastgelegd; over landingsrechten wordt doorgaans bilateraal onderhandeld, terwijl een binnenlandse vlucht sowieso onder de normering van de nationale luchtwet valt. En wie naar de VS en een aantal andere landen wil vliegen, moet als airline een reeks van persoonsgegevens van de passagier verstrekken, voorafgaand aan vertrek.

Het laatste wat soevereine staten willen, is hun jurisdictie afstaan. Dat uitgangspunt is voor de gedigitaliseerde samenleving niet anders en geldt zelfs in versterkte mate nu gegevensverwerking vrijwel onzichtbaar en *at the speed of light* plaatsvindt; nationaal en grensoverschrijdend.