Public Briefing / januari 2014

Een juridische vooruitblik: meer transparantie, waarborgen en zekerheden voor cloud computing onvermijdelijk

Mr. V.A. de Pous[1]

Een juridische toekomstvisie in relatie tot cloud computing hoeft niet beperkt te blijven tot populaire borrelpraat of koffiedikkijken. Onderwerpen staan gewoon op de agenda, terwijl anderen voortvloeien uit analyse van heden en verleden. Een beknopte tour d'horizon.

Wetgeving

Uit Europa verwachten we de vaststelling van de nieuwe Algemene verordening gegevensbescherming. Het gaat om een grondige herziening en actualisering, die bestaande privacyrechten aanscherpt, nieuwe toevoegt en tevens administratieve lasten wil verlichten. Of dat laatste lukt, valt te bezien. Zo zal het ronduit lastig zijn om te becijferen wat de nieuwe Europese meldplicht bij het lekken van persoonsgegevens *in de praktijk* voor overheid en bedrijfsleven betekent, nog los van de dreigende, forse geldboetes op niet-naleving. Tel daarbij op dat we sowieso een toename van wettelijke voorgeschreven meldingen zien voor uiteenlopende incidenten, zoals storingen en datalekken, op basis van het privacyrecht, telecommunicatierecht en andere rechtsgebieden.

'Smalle' meldplichten gelden uitsluitend voor bepaalde sectoren of soorten aanbieders; brede daarentegen, zijn als regel horizontaal van toepassing. De diverse meldingen moeten worden gedaan aan verschillende toezichthouders, zoals het College bescherming persoonsgegevens, Agentschap Telecom of

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

National Cyber Security Centrum (onderdeel van het ministerie van Veiligheid en Justitie). Verwarring ligt hier zowel inhoudelijk en procedureel zeker op de loer. Inhoudelijk uitte bijvoorbeeld de Raad van State forse kritiek op het wetsvoorstel datalekken: te vaag. Justitie is overigens niet van plan de regeling aan te passen.

Rechtstreekse werking

Tenminste van gelijk belang betreft het legislatieve model waarvoor de Europese Commissie expliciet koos. Geen *richtlijn* — die om implementatie in 28 nationale rechtsstelsels vraagt, waardoor onvermijdelijk en ongewenst verschillen per lidstaat ontstaan — maar een *verordening* met rechtstreekse werking. Deze route vormt in feite *de* manier voor het realiseren van een heus geharmoniseerd en uniform wettelijke kader voor de interne markt.

In het domein *cybersecurity* ligt wel een communautaire richtlijn ter tafel. 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 *risicobeheersregelingen* moeten invoeren en tevens — hier hebben we het weer — ernstige incidenten met betrekking tot hun kerndiensten *moeten melden*.

Traditionele visie

Nog een legislatieve ontwikkeling. Dit voorjaar behandelt de Tweede Kamer het wetsvoorstel Computercriminaliteit III, dat onder meer politieambtenaren de bevoegdheid geeft legaal te laten ‘inbreken’ in informatiesystemen. Hierbij passeert de strafvordering een grens van *passief* (observeren, afluisteren, aftappen) naar *actief* handelen, inclusief het plaatsen van malware bij burger en bedrijf; zelfs ongeacht de plaats van de systemen. We voorzien voorafgaand aan vaststelling een scherpe parlementaire behandeling.

Tegelijkertijd laten overheid en politiek zien dat ze problemen ter zake kennelijk alleen traditioneel wil aanpakken. Men staart zich al decennia hoofdzakelijk blind op strafvordering (kort gezegd: telkens meer bevoegdheden voor het opsporingsapparaat), terwijl dezelfde techniek die een forse en escalerende bedreiging vormt, tevens aan preventie kan bijdragen. Betere softwarecode, meer en uitvoeriger testen, mede bij ketenautomatisering, met als resultaat minder kwetsbaarheden en updates.

Digitale kwaliteit juridisch borgen, is een alternatieve route die, zover bekend, nergens ter wereld op de digitale wetgevingsagenda staat.

Faillissementswetgeving

Voor een verrassend wapenfeit zorgt Luxemburg. Naast zijn jarenlange beleid voor een betrouwbare en veilige vestigingsplaats voor de bancaire sector, richt het hertogdom zich nu op datacenters en cloud service providers. Hiertoe wijzigde het onder meer — recent — de faillissementswetgeving. Met een aan zekerheid grenzende waarschijnlijkheid stellen we vast dat Luxemburg het eerste land is waar de curator de wettelijke plicht heeft om in geval van faillissement van clouddienstverlener of hostingsbedrijf de gegevens van de klant onmiddellijk aan de klant te verstrekken, zonder dat deze in een langdurige juridische procedure ter afwikkeling van boedel terecht komt. Dat de regelgeving vrijwel zeker primair op marketinggronden in het leven is geroepen, doet niets aan haar praktische werking af. Andere landen volgen vooralsnog niet.

Cruciaal

Bovenal worstelen gebruikers(organisaties), ICT-leveranciers, en de (niet-Amerikaanse en niet-Engelse) overheid wereldwijd met hetzelfde probleem; zij het van verschillende kanten benaderd. *Vertrouwen in digitale technologie en de informatiemaatschappij met een levensgrote V*. Gebruikers hebben het verloren, de sector moet het bieden; vrijwel zeker samen met het nationale openbaar bestuur. Wat te doen? Het is onvermijdelijk dat — mede in het kader van cloud computing — er meer bilaterale en multilaterale verdragen tot stand komen. Enerzijds gaat het om bescherming van (grond)rechten van staatsburgers, anderzijds om het faciliteren van grensoverschrijdende handel.

In ieder geval neemt de aandacht voor regionalisatie toe. Geopolitieke segmentatie, ook wel de *Balkanization of IT* genoemd, lijkt deels onvermijdelijk. Ook encryptie dringt naar voren, maar of gebruikersorganisaties beseffen dat versleuteling van informatie alleen optimale bescherming biedt wanneer het *key management* in hun handen ligt, valt te betwijfelen. Overigens is zojuist bekend geworden dat de Amerikaanse veiligheidsdienst een quantum computer bouwt om in beginsel iedere vorm van encryptie te kraken.

Nederlandse overheidscloud

Ook ons kabinet richt zich op vertrouwen. In een brief van december aan het parlement meldt zij haar inzet voor een veilig digitaal domein, waarin de kansen van digitalisering worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en de ‘internetvrijheid’ zo optimaal mogelijk worden

beschermd. De voortschrijdende digitalisering van de samenleving heeft namelijk gevolgen voor de economie, de veiligheid en de persoonlijke levenssfeer. Hierop gelet, staat het kabinet in de eerste plaats stil bij de rol die de overheid moet spelen bij de bescherming van persoonsgegevens tegen schendingen door anderen. Zo wordt versneld een *verkenning* — goed beschouwd een haalbaarheidsonderzoek — uitgevoerd naar het opzetten van een Nederlandse clouddienst voor publieke en private vitale processen.

Tot slot

Afsluitend constateren we dat het clouddomein juridisch flink in beweging is. Wetgeving, overheidsbeleid en bijvoorbeeld modelcontracten, waaraan in communautair verband wordt gewerkt. Sommige juridische kaders vloeien voort uit het algemene recht; anderen ontstaan primair voor cloud computing.

Daarnaast stoomt zelfregulering — in de vorm van gedragscodes — op. Nieuw Zeeland *of all places* nam het voortouw. De *New Zealand Cloud Computing Code of Practice* 'is to enable professional cloud service providers to benchmark and demonstrate their practices, processes and ethics via a recognised third party to build trust with prospective customers.' IJkpunt enerzijds en marketingmiddel anderzijds. De code kent verregaande informatieverplichtingen richting klant.

Dan rest ons nog de rechtspraak. Ontstaat er in 2014 eindelijk jurisprudentie over clouddiensten, welke bijvoorbeeld rechten en plichten van contractspartijen nader duiden? Waarschijnlijk wel.