GLOCALISERING

De mondiale cybersecurity-reguleringsgolf

Axel Arnbak

Met de onuitputtelijke mediastorm aan cyberschandalen is 2016 het jaar van de nieuwe cybersecuritywetgeving wereldwijd. China publiceerde onlangs een draconische cybersecuritywet, waar multinationals zich grote zorgen om maken. Vooruitlopend op de eerste integrale Europese cybersecuritywet, medio 2018 van kracht, probeert Nederland nog voor de verkiezingen een nationale versie aan te nemen en zijn de handhavingsboetes voor datalekken alvast sterk verhoogd.

In de Verenigde Staten introduceerde president Barack Obama een federale cybersecuritywet, al is Donald Trump nu aan zet. Ondanks verschillende juridische systemen, spreekt cybersecuritywetgeving gek genoeg één globale taal. Machtsblokken schrijven slechts op details in verschillende accenten. Deze 'glocalisatie' van cybersecurity maakt de toekomst van een urgent rechtsgebied verrassend helder.

Cybersecurity lijkt een politieke hype, maar staat al decennia op beleidsagenda's. Overal — ook in landen als Brazilië, Singapore en Rusland — zie je dezelfde dynamiek: in de jaren negentig begon de regionale sectorregulering, vaak van telecombedrijven. Na een ernstig incident roept de politiek om de eerste, meestal vage, nationale wetgeving voor kritieke IT-infrastructuur zoals energie, banken en ziekenhuizen. Fase drie volgt na een reeks ernstige incidenten; veel striktere 'federale' wetgeving, voor alle marktpartijen, gehandhaafd met hoge boetes. De wettelijke maatregelen zijn mondiaal ook dezelfde. De meldplicht datalekken, de plicht voor bedrijven een intern beveiligingsbeleid te voeren en steeds verdergaande overheidsdwang om informatie inzichtelijk te maken voor politie en inlichtingendiensten. Deze mondiale concepten worden nu vrij homogeen, soms met lokale inkleuring, ingevoerd.

In Europa gold jarenlang een lappendeken van regionale wetjes. In 2008 stapte de EU op de cybertrein met een Europese meldplicht van datalekken voor telecombedrijven. Omdat deze meldplicht in ieder land anders werd geïmplementeerd, en data meestal niet bij telecombedrijven zelf lekken, maar bij andere marktpartijen, bewoog de EU in 2016 naar fase drie met directe wetgeving voor datalekken en hoge boetes.

In de EU gold jaren een lappendeken van regionale wetjes, maar nu is er een Europese meldplicht voor datalekken

Cybersecurity is nieuwer en breder dan privacy, denk aan de continuïteit van de stroomvoorziening en de verknooptheid daarvan met het internet. Met een nieuwe, vage en integrale EU-richtlijn uit 2016 voor kritieke IT-infrastructuur, die lidstaten hopeloos vaag en uiteenlopend zullen implementeren in nationale wetgeving, bevindt de EU zich in fase twee. Na een groot pan-Europees incident zal de EU fase drie introduceren: directe wetgeving met hoge boetes. Onderwijl dwingen alle Europese staten nieuwe internetbevoegdheden af, zoals de sleepnetwet voor de AIVD en de hackwet voor de politie, die in China niet zouden misstaan.

China beweegt zich nu ook naar de tweede reguleringsgolf. De nieuwe wet bevat vooral herkenbare elementen: datalekken, beveiligingsbeleid en meer toezicht. In aanvulling daarop lijkt de wet naar Russisch model multinationals te verplichten Chinese data in China op te slaan en 'betrouwbare' technologie af te nemen, goedgekeurd door de staat. Maar de details zijn onduidelijk en onlangs in Shanghai leerde ik het doel daarvan. In China is geen wet nodig voor overheidsoptreden, maar met de wet creëert China een permanente onzekerheid en dus gehoorzaamheid in de markt. Want met veel bombarie verboden de VS in 2014 producten van Huawei in Amerikaanse overheidssystemen. Amerikaanse techbedrijven krijgen nu een Huawei-koekje van eigen deeg.

In de VS nemen staten al sinds 2002 datalekwetgeving aan, deels in reactie op de reusachtige datalekken bij detailhandel TJ Maxx waarbij 45 miljoen klanten hun creditcarddata verloren. President Obama kondigde in 2015 federale datalekwetgeving aan, fase twee, maar door sluwe Republikeinse oppositie kon Obama de wet niet doorvoeren. En daar is Trump, die ineens de volledige controle krijgt over het Witte Huis, het Congres én het Hooggerechtshof.

Als Trump tijd en zin heeft na het golfen in New Jersey, is fase twee aanstaande. Voor de lokale inkleuring kan Trump de Amerikaanse praktijk van torenhoge schadeclaims laten bestaan, wetten en toezicht naar Europees model inrichten of machtspolitiek naar Chinees model bedrijven. Trumps horoscoop is onvoorspelbaar, maar mondiaal zit cybersecurityregulering stevig in de tweede reguleringsgolf en voor datalekken al in fase drie. Mediastorm of niet, de glocalisering van cybersecurity is een feit en biedt voor multinationals met visie de kans (en plicht) één mondiaal beleid met lokale accenten te voeren.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak