BIG DATA IS DE HYPE VOORBIJ

NIEUWE REGELGEVING LEIDT TOT REALISTISCHER BEELD

Big data leek een synoniem voor gouden bergen. Maar door nieuwe wetgeving wordt de betekenis ervan behoorlijk genuanceerd. Een betoog over de (on)mogelijkheden van big data aan de hand van de meldplicht datalekken en het gebruik van data door inlichtingen- en veiligheidsdiensten.

Tekst: Nico van Eijk, directeur van het Instituut voor Informatierecht

We leven in een informatiesamenleving. Door technologische innovatie, door explosieve groei in communicatie komen meer en meer gegevens beschikbaar. De behoefte om deze data te verzamelen, te gebruiken en te delen neemt exponentieel toe, ook bij de overheid.
Big data, de verzamelterm waaronder dit soort ontwikkelingen wel wordt gevangen, staat midden in de belangstelling en er worden euforische beelden geschetst over wat er allemaal mee mogelijk is. Toenmalig Eurocommissaris Neelie Kroes beschreef in 2013 data als *'the new oil'*. In 2013 stond de olieprijs op bijna 100 euro. Vandaag is die gedaald tot rond de 40 euro.

DATALEKKEN

De enige reden waarom banken werden overvallen was omdat er geld in de kluis lag. Die tijd ligt achter ons. Er is niets meer te halen in een bankgebouw, de kluizen zijn leeg, het geld is gedigitaliseerd. De criminaliteit heeft zich overeenkomstig verplaatst en richt zich op het ontfutselen van toegangscodes (*phishing*) en tot het grootschalig kraken en omzeilen van beveiligingsmaatregelen om zo grote hoeveelheden data te krijgen die voor allerlei vormen van misbruik inzetbaar zijn (creditcard-gegevens, Panamese en Luxemburgse bankgegevens, info op datingsites, et cetera).
Oorspronkelijk bestond de naïeve opvatting dat een en ander een halt kon worden toegeroepen door telecomaanbieders

VERWIJDER WAT NIET STRIKT NODIG IS, HOU DE DATAKLUIZEN ZO LEEG MOGELIJK

De waarde van olie wordt bepaald door vraag en aanbod. Dat is met data niet anders en het is goed om te zien dat er een meer realistisch beeld is over het belang ervan. De toegenomen inbedding van het fenomeen via nieuwe regelgeving draagt daaraan bij.

te verplichten maatregelen te nemen tegen dit soort datalekken. Echter, het probleem bleek niet te liggen bij de aanbieders van telecommunicatienetwerken, maar juist aan de randen ervan: de gebruikers die hun servers, computers en software niet goed beveiligen. Bedrijven, instellingen én overheden als beheerders van grote hoeveelheden data zijn het eerste doelwit.

NIEUWE WETGEVING

Sinds 1 januari is er nieuwe wetgeving over datalekken van kracht. Op de naleving ervan wordt toegezien door de Autoriteit Persoonsgegevens (AP), de nieuwe naam van het College Bescherming Persoonsgegevens (CBP). Deze wetgeving verplicht tot het melden van inbreuken op de beveiliging die leiden tot 'de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'.
Datalekken zijn overigens niet alleen het hacken van websites, maar ook het verlies van usb-sticks met persoonsgegevens valt onder de definitie. De wetgeving gaat er verder van uit dat passende technische maatregelen zijn genomen om datalekken te voorkomen. Er rust hiermee een zorgplicht op de betrokken partijen. In het uiterste geval kan de AP een boete opleggen van 820.000 euro.
In beleidsregels is door de AP nadere invulling gegeven aan de nieuwe bevoegdheden. Door de datalekkenregulering wordt meer concreet duidelijk wat de risico's zijn voor bedrijven, instellingen en overheden. Een actief beleid is onvermijdelijk. Hardware en software

moeten worden geüpgraded naar de norm van 'passende technische maatregelen' en doekjes voor het bloeden zoals excuses aan gebruikers volstaan niet meer. Maar zorgvuldig beleid met betrekking tot datamanagement is eveneens aan de orde. Verwijder en vernietig wat niet strikt nodig is, hou de datakluizen zo leeg mogelijk.

DOOR DE DATALEKKEN-REGULERING WORDT CONCREET DUIDELIJK WAT DE RISICO'S ZIJN VOOR BEDRIJVEN, INSTELLINGEN EN OVERHEDEN

NATIONALE VEILIGHEID

In een cartoon zegt een jongetje tegen Obama: *'Dad says you're spying us online'*, waarop Obama antwoordt: *'He's not your dad.'* De onthullingen van Snowden geven niet alleen aan op wat voor schaal data worden verzameld door overheden in het belang van nationale veiligheid, maar ook wat voor gebruik en misbruik daarvan wordt gemaakt of kan worden gemaakt.

Het zeker stellen van de rechtsstaat is een groot goed en inlichtingendiensten dragen daaraan bij. Momenteel ligt een wetsvoorstel voor een nieuwe wet op de inlichtingen en veiligheidsdiensten (Wiv) ter advisering bij de Raad van State. Het omvat twee grote veranderingen ten opzichte van de huidige wetgeving, die beide zijn ingegeven door de nieuwe mogelijkheden om digitale informatie te gebruiken. In de eerste plaats wordt de wetgeving technologieneutraal gemaakt. Zo laat de bestaande Wiv alleen toe dat draadloze informatie massaal wordt vergaard, de nieuwe breidt dit uit naar vaste infrastructuur.

KRITIEKPUNTEN

Dat het wetsvoorstel aldus *'mass surveillance'* mogelijk maakt is een van de belangrijkste kritiekpunten. Bovendien richt de wet zich niet meer alleen op traditionele telecommunicatie, maar vallen ook sociale mediadiensten als Facebook of Twitter en alternatieve communicatiediensten (Whatsapp, Skype, et cetera) onder de reikwijdte van de wet.

Bij zulke verstrekkende bevoegdheden hoort de hoogst mogelijke zorgvuldigheid bij het inzetten ervan en zeer effectief toezicht. De inzet van middelen, zo schrijft de concepttekst voor, moet telkens getoetst worden aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Een middel hoort daadwerkelijk en effectief bij te dragen aan het beoogde doel en telkens moet het minst verstrekkende middel worden ingezet.
'Mass surveillance' zal bijvoorbeeld alleen in bijzondere gevallen – als andere minder vergaande maatregelen falen – mogen worden ingezet omdat het primair gaat om het verzamelen van gegevens van onschuldige burgers. Maar ook het stelselmatig verzamelen van gegevens via openbare bronnen (Twitter/Facebook) mag alleen met toestemming.

VERBETERING TOEZICHT

In een aantal recente uitspraken hebben Europese rechters (het Hof van Justitie in Luxemburg en het Europese Hof voor de Rechten van de Mens in Straatsburg) duidelijk een halt toegeroepen voor wat betreft het ongebreideld inzetten van digitale opsporingsmethodes.
Het zijn deze rechters die eveneens aan de basis liggen van de tweede belangrijke wijziging: de verbetering van het toezicht. De bestaande Wiv kent alleen de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). Deze commissie is beperkt tot het achteraf beoordelen van door de minister goedgekeurde maatregelen en het daarover rapporteren.
De CTIVD heeft geen handhavingsbevoegdheden. Dit is ten enenmale onvoldoende, zo volgt uit Europese maar ook nationale jurisprudentie. Het toezicht moet effectief zijn en beoogde maatregelen vooraf kunnen worden goedgekeurd of verworpen.

Nico van Eijk: Big data ontstijgt de hype

DE INZET VAN MIDDELEN MOET TELKENS GETOETST WORDEN AAN EISEN VAN NOODZAKELIJKHEID, PROPORTIONALITEIT EN SUBSIDIARITEIT

NIEUWE BALANS

Dit is eigenlijk niets nieuws. Oorspronkelijk was al geregeld dat de interceptie van alle vormen van toenmalige grootschalige communicatie vooraf de instemming van de rechter moesten hebben: het briefgeheim. Dit beginsel wordt in het voorstel hersteld zij het dat er deels een bevoegdheid komt bij de rechtbank Den Haag (voor communicatie betreffende het brongeheim van journalisten, het raadsman/cliënt privilege voor advocaten en voor het briefgeheim) en deels bij een nieuwe toetsingscommissie (voor overige toestemmingen). Dit is vragen om complicaties en er is geen duidelijke reden waarom niet in alle gevallen de rechter bevoegd kan zijn.
Het voorstel voor een nieuwe Wiv beoogt een nieuwe balans te vinden tussen informatievergaring en de beperkingen alsmede het toezicht daarop. Er valt nog het nodige in de tekst te verbeteren en hopelijk zal dat ook gebeuren: eerst maar eens zien wat het advies van de Raad van State brengt.

BIJZONDER BELANG

Laat duidelijk zijn dat de Wiv geen reden is om ook elders binnen de overheid voor gelijke mogelijkheden te pleiten. De ruime bevoegdheden van de Wiv zijn ingegeven door het bijzondere belang van de nationale veiligheid. Dat is niet gelijk te stellen met reguliere strafvordering of de handhaving van socialezekerheidswetgeving. Andere overheden zijn gebonden aan de gewone privacyregulering, die zeer strikt is ten aanzien van het gebruik van persoonsgegevens en in beginsel geen ruimte laat voor 'mass surveillance'.
Recent onderzoek van de AP leverde op dat gemeenten onvoldoende op de hoogte zijn van wat voor regels gelden voor het verwerken van gegevens in het sociaal domein (waartoe onder meer jeugdzorg, maatschappelijke ondersteuning en arbeidsparticipatie vallen). In het kader van hun publieke taak hebben overheden in de wet geregelde mogelijkheden om persoonsgegevens te verwerken, maar waar dat niet het geval is dienen zij pas op de plaats te maken. Aan burgers toestemming vragen wanneer er geen wettelijk kader is helpt niet, omdat burgers vrij toestemming moeten kunnen geven en dat is bij overheden niet mogelijk mede vanwege de afhankelijke/hiërarchische relatie tussen overheden en burgers.

CHECKS EN BALANCES

Big data ontstijgt de hype. Mogelijkheden en risico's worden steeds beter zichtbaar. Nu klassieke beperkingen als technologische complexiteit en kosten zijn weggevallen, dienen nieuwe checks en balances te worden gevonden. Overheden hebben hier een bijzondere verantwoordelijkheid omdat zij zowel verzamelaar en gebruiker zijn, maar ook moeten instaan voor de naleving van de rechten van burgers inzake privacy en dataprotectie. Dat overheden bewust of onbewust burgers gaan bespioneren omdat de digitale wereld dat zo gemakkelijk maakt draagt sowieso niet bij aan de vaak toch al broze vertrouwensrelatie tussen burgers en overheden.