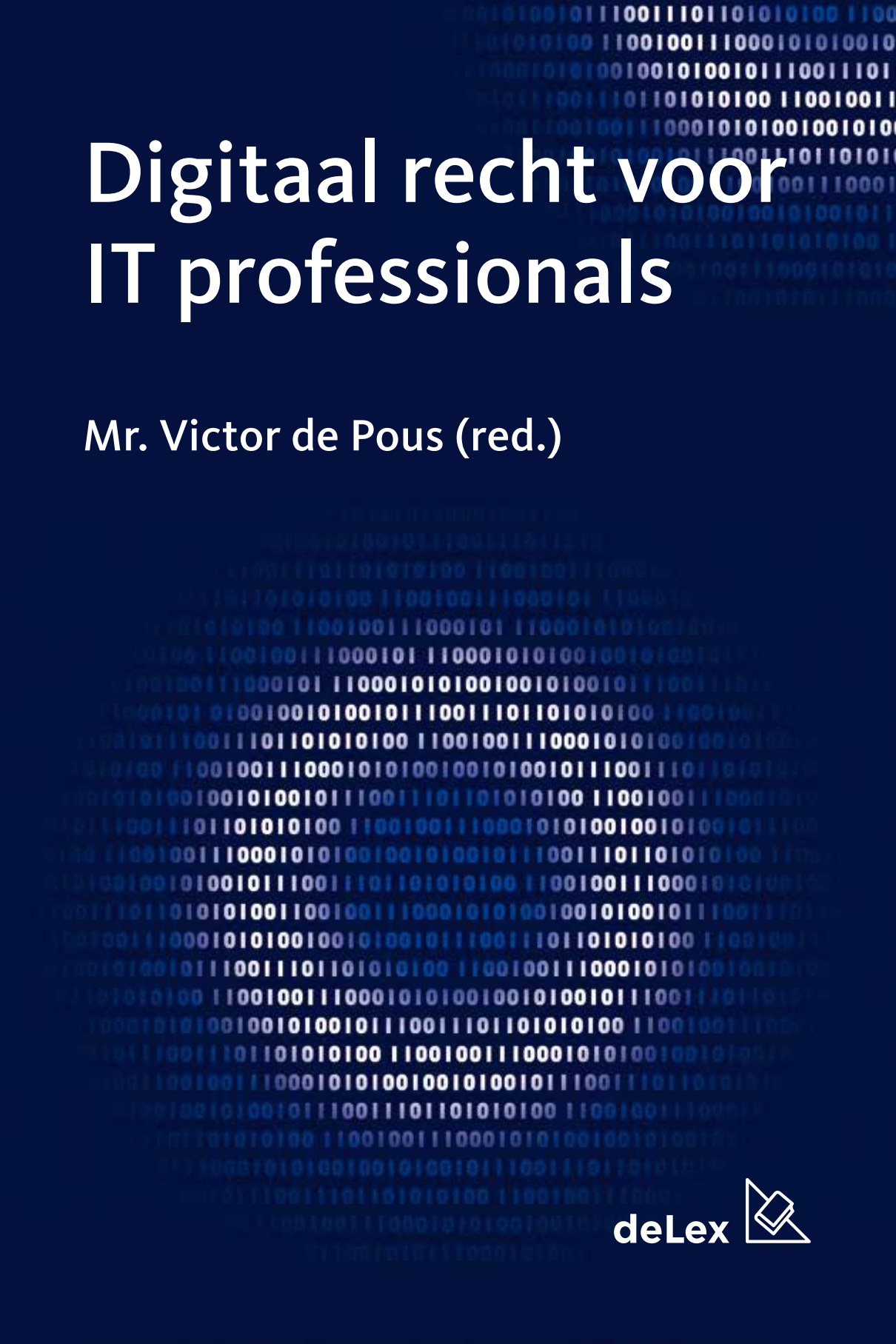
Digitaal recht voor IT professionals

Mr. Victor de Pous (red.)



deLex

Digitaal recht voor IT professionals

30 jaar Ngi-NGN Special Interest Group IT en Recht

Digitaal recht voor IT professionals

30 jaar Ngi-NGN Special Interest Group IT en Recht

Victor de Pous (red.)

deLex

© 2016, G. Boudewijn, N.H.A. van Duuren, J. Honkoop, R. van Houten, K. Konings, P.W.M. Oor, S. van Otterloo, V.A. de Pous, I.P.V. van Schelven, P.C. van Schelven, E.P. Tamminga, L.L.A.M. Thissen en S.R. Wallagh.

ISBN: 978-90-8692-061-7
NUR: 820

Ontwerp omslag en binnenwerk: az grafisch serviceburo, www.az-gsb.nl

Uitgeverij deLex
www.deLex.nl

7 Encryptie

Serge Wallagh

Het gebruik van versleuteling om digitale gegevens te beveiligen, staat volop in de politieke en juridische belangstelling. Terwijl de Nederlandse regering een stevig standpunt *voor* heeft ingenomen, willen Frankrijk en Duitsland juist met het oog op de bestrijding van terrorisme onder voorwaarden bij beschermde gegevens kunnen. Met de huidige stand der techniek van encryptiemethoden is het mogelijk om gegevens dusdanig te beveiligen, dat het redelijkerwijs niet meer mogelijk is voor onbevoegden om zonder sleutel, de versleutelde gegevens in te kunnen zien. Voor gebruikersorganisaties lijkt encryptie een mooie uitweg, om je niet druk te hoeven maken over de beschermingsvoorschriften van de Wet Bescherming Persoonsgegevens, inclusief de regels van Wet Meldplicht Datalekken, die sinds 1 januari 2016 van de Wbp een onderdeel vormt. Is deze hypothese valide? Daarnaast rijst de vraag of er beperkende rechtskaders voor digitale versleuteling zijn. Anders gezegd, mag encryptie onbeperkt worden ingezet? En zo ja, welke garanties biedt dat dan?

Onbeperktheid

In 2012 was er een wetsvoorstel in de maak die verdachten van ernstige feiten, zou verplichten mee te werken bij het openen van versleutelde bestanden.[65] Dat wetsvoorstel is er niet gekomen en de mening van het kabinet wijzigde nogal. De ministers van Veiligheid en Justitie en Economische zaken meldden begin dit jaar aan de Tweede Kamer dat het kabinet het onwenselijk vindt 'om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland'.[66] In Nederland kan de politie dus niet eisen dat iemand, of een leverancier, meewerkt aan het ontsleutelen van gegevens.[67] De regering wil dit standpunt tevens internationaal verkondigen.

Internationaal wordt immers sterk verdeeld gedacht over het onbeperkt gebruik van encryptie. Juridisch zijn er dus geen beperkingen voor het gebruik van sterke encryptie.

65 Wetsvoorstel computercriminaliteit III.

66 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie.

67 Vergelijk FBI-Apple casus https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute.

Maar dat niet iedereen het hier mee eens is, blijkt wel uit het feit dat de directeur van de AIVD ervoor pleit dat men encryptie van chatdiensten als Telegram, WhatsApp en Signal moet beperken. Het is volgens hem essentieel voor het beschermen van de rechtsorde om de communicatie van verdachte personen te ontsleutelen.[68] Men kan trouwens vraagtekens zetten bij *nationaal* beleid op dit punt, aangezien veel dataverkeer juist internationaal zal zijn. Welke regels gelden dan?

Wet Bescherming Persoonsgegevens

Centraal in de WPB staat het begrip *persoonsgegeven*. De wet bepaalt: 'Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[69] Deze omschrijving roept de vraag op of een versleuteld persoonsgegeven, ook (nog) een persoonsgegeven is in de zin van de wet. Ofwel, gelden de regels van de WBP voor *encrypted data*? Wij beantwoorden de rechtsvraag positief. In de beleidsregels voor de nieuwe meldplicht datalekken, die sinds 1 januari 2016 geldt, stellen de Autoriteit Persoonsgegevens eenduidig dat: 'Als verantwoordelijke bent u, ook na de encryptie of hashing, nog steeds in staat om de betrokkene te identificeren. Er is dus nog steeds sprake van persoonsgegevens.'[70] Volgens de toezichthouder geeft encryptie dus geen *cart blanche* om met gegevens te doen wat men wil, maar helpt wel de impact te voorkomen bij dataverlies. Indien er passende technische beschermingsmaatregelen zijn [...] kan melding aan de betrokkene achterwege gelaten worden.[71] Simpel gezegd: bij gegevensverlies met encryptie hoeft men niet met de billen bloot richting de betrokkenen.

Eerst een geruststelling. Op basis van de huidige stand van technologie kunnen we de aanname doen dat het uitwisselen van gegevens via internet of andere wegen dusdanig te beveiligen valt, dat de kans op diefstal van (bruikbare) gegevens tijdens de uitwisseling voldoende klein is. Daar hoeven we ons dus niet meer echt druk om te maken. Het wordt echter ingewikkeld als men met de gegevens echt iets wil doen. Het sleutelbeheer vormt dan zowel technisch, organisatorisch als ook juridisch de Achilleshiel van encryptie. Een juridisch belangrijke vraag bij encryptie is daarom: '*waar* gebeurt de encryptie echt en *wie* heeft de sleutel?' De exacte locatie van de versleuteling kan in de praktijk directe juridische consequenties hebben. Hierbij zien we ruwweg twee scenario's.

68 Volkskrant 17-9-2016, interview met AIVD-directeur Rob Bertholee.

69 Artikel 1 lid, a Wbp.

70 https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-beleidsregels-meldplicht-datalekken.

71 Artikel 34a, zesde lid, Wbp.

Ten eerste: *client-side encryption*

In dit scenario's gebeurt encryptie door de gebruiker zelf, op de PC van de gebruiker. Deze werkwijze wordt 'client-side encryptie' genoemd. Dit was bijvoorbeeld het geval in de zaak Robert M., waarbij kinderporno versleuteld op de computer van Robert M. stond.[72] De versleutelde gegevens worden vervolgens verstuurd naar een verwerker. Denk bijvoorbeeld aan een cloudleverancier. De bewerker slaat de gegevens op en stuurt ze desgewenst terug naar de gebruiker; of naar andere gebruikers. Alleen gebruikers die de (geheime) sleutel weten, kunnen de gegevens vervolgens ontsleutelen. Voordeel is dat bij een datalek bij de bewerker nooit de sleutels verloren kunnen gaan, want de bewerker heeft geen sleutel. Het essentiële nadeel van deze werkwijze betreft dat de bewerker – omdat hij geen sleutel heeft – niets met de gegevens doet. Inzage in de versleutelde bestanden is niet mogelijk, evenals het uitvoeren van zinvolle bewerkingen. Goed beschouwd leent zich client-side encryptie in beginsel uitsluitend voor archivering en online back-up.

Ten tweede: *server side encryption*

In de meeste gevallen willen we dat de bewerker juist wel 'iets' met de gegevens kan doen. Een gebruikersorganisatie stuurt bijvoorbeeld gegevens 'leesbaar' door naar een leverancier van clouddiensten.

De cloudleverancier als bewerking in de zin van Wet bescherming persoonsgegevens bewerkt de gegevens en slaat ze vervolgens versleuteld op. De bewerker kan echter zelf de gegevens weer ontsleutelen, zodra er een bewerking nodig is. Alle Software-as-a-Service leveranciers werken (maximaal) op deze manier, omdat ze om hun dienst aan te bieden de gebruikersgegevens niet alleen moeten opslaan, maar uiteraard ook zinvol moeten kunnen bewerken, zoals bijvoorbeeld bij Microsoft Officce 365.[73] Er geldt nou eenmaal: men kan geen boek samenvatten, zonder de taal waarin het geschreven is te begrijpen. Dit betekent dus voor de eigenaar van de gegevens dat een volledige veiligheid niet meer te garanderen is: men moet een derde partij vertrouwen met toegang tot de onversleutelde gegevens. Bij een datalek aan de kant van de bewerker, is daarmee onmogelijk aan te geven in hoeverre er sprake is van verspreiding. Dit is helaas niet een heel uitzonderlijke situatie: uit recent onderzoek door de Cloud Security Alliance blijkt dat 59% van de klanten van cloud leveranciers incidenten heeft gehad waarbij gegevens ongewild extern zijn verspreid[74]. Men zal in zo'n geval dus meestal wel alle betrokkenen moeten waarschuwen.

Encryptie biedt verder nog unieke mogelijkheden om de juridische bewijskracht van een bericht sterk te vergroten. Met encryptie kan men zorgen dat van een

72 https://nl.wikipedia.org/wiki/Amsterdamse_zedenzaak.

73 https://www.microsoft.com/en-us/TrustCenter/Security/Encryption.

74 *Mitigating risks for cloud applications*, Cloud Secuirty Alliance, 2016.

bericht onweerlegbaar vaststaat wie de afzender is via een gekwalificeerde elektronische handtekening[75].

Conclusie

De versleuteling van persoonsgegevens biedt voor een gebruikersorganisatie *niet* de mogelijkheid om onder alle voorschriften van de Wet bescherming persoonsgegevens uit te komen, maar *wel* voor een deel van de verplichtingen op grond van de Wet meldplicht datalekken. Daarnaast kan encryptie de bewijskracht van gegevens sterk verhogen. Encryptie vormt dus een noodzakelijk onderdeel van een gegevensbeveiligingsstrategie, maar is helaas niet het totale antwoord.

Aandachtspunten

- Encryptie is een volwassen technologie. Organisaties zouden het zoveel mogelijk moeten gebruiken, omdat het (ondanks alle beperkingen) een flinke dam opwerpt tegen misbruik van de gegevens en helpt met de juridische bewijskracht van de gegevens.
- Het kabinet vindt beperking van encryptie 'op dit moment niet wenselijk'. Er geldt momenteel dus geen beperking aan het gebruik van encryptie *in Nederland*. Voor internationaal gebruik is de situatie een stuk onduidelijker. Bedrijven moeten internationaal er rekening mee houden dat er wel beperkingen kunnen (gaan) gelden.
- De technische middelen voor het *uitwisselen* van gegevens zijn dusdanig veilig, dat dit in de praktijk niet vaak tot datalekken zal leiden.
- Client-side encryptie kan in sommige scenario's daadwerkelijk een 100% oplossing bieden, zodat encryptie in deze scenario's eigenlijk altijd toegepast zou moeten worden.
- Daarentegen kan *server-side encryptie* in beginsel nooit sluitende oplossingen voor privacyvraagstukken bieden. Het feit dat de bewerker de gegevens kan lezen (omdat hij noodzakelijkerwijs de sleutels heeft), maakt dat het geen volledige veilige oplossing is. In geval van een groot datalek zal de gebruikersorganisatie ook met *server-side encryptie* veelal niet onder de meldplicht richting de betrokkenen uitkomen.
- Encryptie kan ook gebruikt worden om de bewijskracht van data sterk te vergroten. Het digitaal ondertekenen van documenten, op basis van encryptie, is al lang technisch mogelijk maar wordt (te) weinig gebruikt. Bedrijven zouden deze technologieën veel meer moeten gaan gebruiken.

75 https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening.

Wie denkt dat recht voor juristen bedoeld is, slaat de plank mis. Juridische normering richt zich namelijk primair op dat deel van de samenleving dat het beoogt te regelen. Neem het wegenverkeersrecht. Een automobilist behoort tijdens het besturen zelf de verkeersregels toe te passen. Achteraf op de compliance-kennis van de juridische dienst van verzekeraar of eigen bedrijf vertrouwen, biedt weinig soelaas bij het voorkomen van verkeersovertreding of ongeval. Een wellicht flauwe, maar daarom niet minder treffende constatering. Ook de noodzaak tot het verwerven van begrip en kennis van digitaal recht door leken, in het bijzonder de IT professional, staat buiten kijf. Bovendien hoort digitaal recht tenminste op hoofdlijnen thuis in de bestuurskamer van ieder bedrijf en overheidsorganisatie, omdat dit rechtsgebied het fundament vormt voor – besturen en ondernemen in – informatiesamenleving en *single digital market*. Dat geldt zo mogelijk in het bijzonder voor ICT-bedrijven, die vanouds zowel aan inkoop- als verkoopkant bits en bytes in hun DNA hebben.

De unieke bundel, geschreven, samengesteld en uitgegeven ter gelegenheid van het dertigjarig jubileum van Ngi-NGN Special Interest Group IT en Recht (ooit gestart als Afdeling Computerrecht van het Nederlands Genootschap voor Informatica) in november 2016, bevat dertig artikelen, speciaal geschreven voor de beroeps-ontwikkeling van IT professionals. De handzame publicatie is tegelijkertijd zeker niet beperkt tot deze doelgroep. Ook anderen kunnen hiermee hun voordeel doen. Het gaat immers om belangrijke rechtsontwikkelingen voor *alle* niet-juristen. De juridische onderwerpen lopen samengevat uiteen van privacy tot software-ontwikkeling, van online-handel tot eHealth, van slimme steden tot sjoemel-software, van verzekering tot sociale media, van encryptie tot criminaliteit, van cookies tot fintech, van cloud computing tot big data, van mislukte automatisering tot conflictoplossing, en meer.

Één zaak is duidelijk. De juridische aspecten van computers zijn in dertig jaar tijd van een pril en exotisch onderdeel van het recht tot een breed en cruciaal rechtsdomein geëvolueerd, dat de basis vormt voor onze moderne informatie-maatschappij. Aan deze rechtsontwikkeling komt vooralsnog geen einde.
Blijf het ICT-recht dus volgen.

9 789086 920617

deLex

Ngi nNG
Platform voor
IT-professionals