Privacy, de vijfde golf en de tweede wet van de thermodynamica

Edo Roos Lindgreen

1. Inleiding

In 1948 schreef George Orwell zijn roman 1984. Iedereen kent het verhaal. Een almachtige staat houdt alles en iedereen voortdurend in de gaten. Privacy bestaat niet meer. In 1984 debatteerden we al over het opslaan en uitwisselen van persoonsgegevens en de gevolgen van automatisering voor privacy. Anno 2011 is het onderwerp actueler dan ooit. De definitie van privacy is niet veranderd, maar de perceptie ervan wel, en ook de omstandigheden die op privacy van invloed zijn: van cameratoezicht, klantprofilering en het aftappen van internet- en telefoonverkeer tot het verkopen van persoonsgegevens, het opnemen van digitale vingerafdrukken in het paspoort en het massale gebruik van sociale media. Dat privacy onder druk zou komen te staan hadden wij in 1984 wel bedacht, maar niet op deze manier en zeker niet in deze mate. De vraag is hoe het op dit moment met onze privacy is gesteld en hoe we in de toekomst tegen het onderwerp zullen aankijken.

Dit artikel gaat in op de verschillende dimensies die aan het privacyvraagstuk zijn verbonden. Vervolgens wordt ingegaan op de relatie tussen beheersing en openbaarheid. Tenslotte wordt een verwachting uitgesproken over de gevolgen van technologische en sociaal-economische ontwikkelingen op het begrip privacy en onze perceptie daarvan.

2. Dimensies van privacy

Het privacyvraagstuk kent ten minste een juridische, een technologische en een sociaal-economische dimensie. Deze dimensies komen hieronder kort aan de orde.

2.1 Juridische dimensie

De juridische dimensie van privacy lijkt simpel en solide. Privacy is een fundamenteel recht dat is verankerd in de Europese privacyrichtlijn 95/46/EG en in artikel 10 van onze Grondwet:

> Artikel 10
>
> 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
>
> 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
>
> 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Dit artikel is weer verder uitgewerkt in de Wet bescherming persoonsgegevens (Wbp), die sinds 1 september 2001 van kracht is. De wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de plichten zijn van de instanties of bedrijven die gegevens gebruiken.

De Wbp stelt eisen aan de verwerking van persoonsgegevens. Een organisatie mag persoonsgegevens alleen verzamelen en verwerken als daar een goede reden voor is, of als de betrokken burger toestemming heeft gegeven voor het gebruik van zijn gegevens; mag niet meer gegevens verwerken dan strikt noodzakelijk is voor het doel waarvoor ze zijn verzameld; mag de gegevens niet langer bewaren dan noodzakelijk; moet passende technische en organisatorische maatregelen treffen om de gegevens te beschermen; moet de verwerking in veel gevallen melden; moet de betrokken burger in principe altijd informeren over de gegevensverwerking. Het onafhankelijke College Bescherming Persoonsgegevens (CBP) houdt toezicht op de naleving van deze en andere wetten die het gebruik van persoonsgegevens regelen.[1]

De juridische as is echter minder stabiel dan hij lijkt. De Tweede Kamer behandelt met grote regelmaat wetsvoorstellen die de opslag, internationale uitwisseling en toegankelijkheid van persoonsgegevens beogen uit te breiden (dit in het kader van misdaad- en terrorismebestrijding) en daarmee op enige wijze de privacy aantasten. Handhaving van de bestaande privacywetgeving blijkt in de praktijk zo goed als onmogelijk door het aantal persoonsgegevens dat in omloop is en het aantal internationale en soms ongrijpbare partijen dat daarbij betrokken is. En intussen roepen rechtsgeleerden op tot een herbezinning, onder meer omdat de huidige juridische definitie van privacy en de interpretatie daarvan kunnen leiden tot de aantasting van andere grondrechten, zoals de vrijheid van meningsuiting en informatievergaring, die onder meer is vastgelegd in artikel 10 van het Europese Verdrag van de Rechten van de Mens.[2]

Kortom, hoe goed privacy ook in richtlijnen en grondwetten is verankerd, de uitwerking in nationale wetgeving en de handhaving van die wetgeving in de dagelijkse praktijk staan onder voortdurende druk.

2.2 Technologische dimensie

De technologische dimensie is veel veranderlijker dan de juridische. Op het moment van schrijven bevinden wij ons in wat de vijfde golf van IT-innovatie wordt genoemd, na het mainframe, de minicomputer, de personal computer en het internet. Kenmerkend voor deze vijfde golf zijn smartphones, tablets, cloud computing en social media.

Van smartphones en tablets zijn inmiddels honderden miljoenen exemplaren verkocht. Ze zijn verantwoordelijk voor het ontstaan van een compleet nieuwe industrie. Smartphones gaan hand in hand met cloud computing. Hierbij brengen organisaties de verwerking en opslag van hun gegevens naar “the cloud”: goedkope en vrijwel onbeperkte capaciteit die via internet beschikbaar is. Cloud-diensten worden aangeboden door groot en sterk groeiend aantal providers en onderaannemers die

[1] www.cbpweb.nl
[2] Van Hoboken, J. (2009). Privacy in het digitale tijdperk. Opening academisch jaar. Universiteit van Amsterdam. 30 augustus 2009.

vaak samenwerken in ketens en met wie vaak lastig afspraken te maken zijn. De gebruiker verliest hiermee feitelijk de controle over zijn eigen gegevens. Hij kan weliswaar van alles met die gegevens doen, maar hij heeft geen idee waar ze zich bevinden en wie er nog meer bij kunnen. Tenslotte social media. Marktleider Facebook is de afgelopen jaren explosief gegroeid en heeft in 2012 meer dan 1 miljard actieve gebruikers die de meest persoonlijke informatie met elkaar uitwisselen. Door Facebook is de wereld een orde van grootte kleiner geworden; de gemiddelde afstand tussen twee personen is gedaald van 6 kennissen naar 4,75[3]. Leveranciers van smartphones, cloud-diensten en social media als Apple, Google en Facebook beschikken inmiddels over persoonsgegevens van honderden miljoenen mensen.

In 1984 waren gegevens opgeslagen op centrale computers in afgeschermde bunkers. Gegevens waren alleen toegankelijk voor een kleine kring gebruikers. Tegenwoordig biedt het technologische landschap een andere aanblik. Gegevens zijn niet meer eenmalig opgeslagen, maar vele malen, en ze zijn verspreid over talloze verschillende componenten, van mainframes en internetservers tot mobiele telefoons en minuscule geheugenkaartjes die op een heleboel verschillende manieren toegankelijk zijn. Volgens de wet van Moore[4] wordt de dichtheid van transistoren op een geïntegreerd circuit elke achttien maanden grofweg twee keer zo groot, en daarmee ook de rekenkracht, opslagcapaciteit en communicatiebandbreedte van informatietechnologie). Dit exponentiële groeitempo leidt tot effecten die blijven verbazen. In 1984 was de Cray X-MP de krachtigste supercomputer ter wereld. Hij kostte veertig miljoen gulden. Een Apple iPhone kost nog geen 400 euro en is krachtiger dan de Cray. Van de Cray zijn enkele tientallen exemplaren verkocht, van de iPhone honderden miljoenen. Dat deze ontwikkelingen hun weerslag hebben op informatiebeveiliging en privacy moge duidelijk zijn. Steeds meer persoonsgegevens worden opgeslagen en verwerkt op steeds meer, steeds kleinere en steeds krachtiger componenten die zowel individueel als collectief steeds moeilijker te beschermen zijn. De wet van Moore zal nog wel even van kracht blijven. Extrapolerend is de verwachting gerechtvaardigd dat wij over 25 jaar dagelijks gebruikmaken van nauwelijks beveiligde componenten met de kracht van een Cray X-MP en de fysieke omvang, het energieverbruik en de prijs van een broodkruimel. Hiervan zullen geen tientallen, geen honderden miljoenen, maar tientallen miljarden exemplaren in omloop zijn.

Informatietechnologie zal zich de komende decennia in een moordend tempo blijven ontwikkelen en dat die ontwikkelingen de bescherming van persoonsgegevens niet gemakkelijker zullen maken, maar juist moeilijker.

2.3 Sociaal-economische dimensie

Dan de sociaal-economische dimensie. Deze dimensie hangt sterk samen met de waarde van persoonsgegevens, of de perceptie daarvan. De belangrijkste ontwikkeling langs deze dimensie is dat consumenten en burgers op dit moment de economische

[3] Backstrom, L. et. al. (2011). Four Degrees of Separation. arXiv:11114570v1 [cs.SI] 19 November 2011.
[4] Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics*. Volume 38, Number 8.

waarde van hun persoonsgegevens systematisch lager inschatten dan bedrijven en overheden.

Bedrijven hebben veel geld over voor de profielen van consumenten – wie zijn klant kent, heeft de markt. Een goed klantprofiel kan in de huidige markt vele euro's opleveren. Sommige bedrijven maken misbruik van deze situatie. Zij verzamelen persoonsgegevens en verkopen deze door aan derden zonder toestemming van de betrokkenen. Een recent voorbeeld is het schenden van privacy door een Nederlands internetbedrijf Advance. Het CBP rapporteert hierover (citaat): "Het CBP concludeert na onderzoek dat het bedrijf Advance de wet heeft overtreden door via internetplatforms gevoelige gegevens te verzamelen van mensen en vervolgens hun geprofileerde persoonsgegevens aan derden te verkopen zonder de betrokkenen hierover duidelijk en volledig te informeren. Circa 2,2 miljoen mensen nemen deel aan de internettests van Advance. Advance biedt de mogelijkheid op internet een test in te vullen om bijvoorbeeld 'je echte leeftijd' te achterhalen. Uit het onderzoek blijkt dat Advance persoonsgegevens heeft gecombineerd met kenmerken die zijn afgeleid uit de antwoorden op de vragen van de internettests en deze geprofileerde gegevens vervolgens aan derden heeft verkocht. Ook heeft Advance de antwoorden op de tests gebruikt om groepen mensen te selecteren voor zogeheten hostmailings in opdracht van derde partijen. Uit het onderzoek blijkt bovendien dat Advance zeer gevoelige gegevens, zoals medische gegevens, heeft verzameld en verwerkt, terwijl hiervoor in beginsel een wettelijk verbod geldt. Advance heeft de betrokkenen van al dit gebruik van hun gegevens niet volgens de wettelijke eisen geïnformeerd."[5]

Ook overheden hechten grote waarde aan persoonsgegevens, niet uit commerciële overwegingen, maar vooral voor het bestrijden van fraude, terrorisme en andere vormen van criminaliteit. Hoe groot die waarde is, blijkt onder meer uit gegevens over afgeluisterd internet- en telefoonverkeer. Per jaar tapt de overheid tienduizenden telefoongesprekken en het verkeer van honderden internetgebruikers af.[6] Hiermee zijn investeringen van vele tientallen miljoenen euro's gemoeid, zowel bij de aanbieders (die de gegevens moeten bewaren) als bij de overheid (die de gegevens gebruikt). Ook het combineren van gegevens in de bestanden van bedrijven en instellingen, het analyseren van betaalstromen, het in kaart brengen van verkeers- en vervoersgegevens en cameratoezicht zijn essentiële instrumenten geworden in het arsenaal van de opsporingsdiensten en inlichtingen- en veiligheidsdiensten. Cameratoezicht heeft een ongekende vlucht genomen. Het Verenigd Koninkrijk heeft naar schatting 1 beveiligingscamera per 14 inwoners; andere Europese landen doen hier niet voor onder.[7] Camerabeelden worden in toenemende mate gekoppeld aan beeldherkenning zodat deze herleidbaar zijn tot natuurlijke personen.

Voor bedrijven en overheden zijn persoonsgegevens dus zeer waardevol.

Tegelijkertijd lijkt het belang van privacy voor de burger – en daarmee de waarde die men toekent aan de eigen persoonsgegevens – alleen maar af te nemen. Honderden miljoenen gebruikers van sociale media geven zeer intieme gegevens prijs zonder dat daar enige tegenprestatie tegenover staat. Met 1 miljard actieve gebruikers en een

[5] College Bescherming Persoonsgegevens, persbericht, 18 december 2009
[6] Ministerie van Justitie, Vragen naar aanleiding van een schriftelijk overleg inzake tapstatistieken (30517), 2 september 2009
[7] London Evening Standard, 31 maart 2007

geschatte beurswaarde van 100 miljard dollar is de huidige waarde van een Facebook-profiel ongeveer honderd dollar. Sommige sociale media brengen zelfs bedragen in rekening aan de gebruiker. In het denken over privacy lijkt de afgelopen 25 jaar zo een grote wijziging te hebben plaatsgevonden, die zich het sterkst manifesteert bij de generatie die opgroeit met internet als normaal bestanddeel van het dagelijkse leven.

3. Het vierde kwadrant

Welke gevolgen heeft deze cocktail van technologische vooruitgang en sociaal-economische ontwikkelingen nu voor het onderwerp privacy? Bij het beantwoorden van deze vraag kunnen we kijken naar de kring waarbinnen de gegevens worden verspreid (van volledige beslotenheid tot volledige openbaarheid) en naar de mate waarin de betrokkene zelf controle kan uitoefenen over zijn of haar gegevens (van volledige controle tot een volledig gebrek aan controle).

Deze aspecten *verspreiding* en *beheersing* vormen samen een vlak dat we voor het gemak kunnen indelen in vier kwadranten, zie onderstaande figuur.

In het eerste kwadrant linksonder heeft de betrokkene controle over zijn of haar persoonlijke gegevens en worden die gegevens uitsluitend in een besloten omgeving gebruikt. Voorbeelden hiervan zijn bestanden op de eigen computer, foto's en filmpjes op een mobiele telefoon, maar ook de vastlegging van het gebruik van bonuskaart, tankpas en OV-chipkaart.

In het tweede kwadrant linksboven heeft de betrokkene ook controle over zijn of haar persoonlijke gegevens, maar worden deze gegevens bewust openbaargemaakt. Voorbeelden zijn persoonlijke pagina's op sociale media als Facebook of LinkedIn. De opkomst van deze sociale media heeft geleid tot een massale publicatie van persoonlijke gegevens op internet; niet alleen gewenst en bewust, maar vaak ongewenst of onbewust.

In het derde kwadrant rechtsonder zitten persoonlijke gegevens in een besloten omgeving waar de betrokkene niet of nauwelijks controle over heeft. Vaak is hij of zij niet eens op de hoogte van het bestaan van deze gegevens. Voorbeelden zijn de databases van marketingbureaus en inlichtingendiensten, maar ook de beelden van beveiligingscamera's en filmpjes op de mobiele telefoons van anderen. We leven onder permanent cameratoezicht, niet van Orwell's Big Brother, maar van een heleboel kleine broertjes en zusjes.

Het laatste kwadrant rechtsboven is de oncontroleerbare openbare ruimte. In dit kwadrant zijn persoonlijke gegevens volledig openbaar en zijn ze niet of nauwelijks door de betrokkene zelf te beïnvloeden. Voorbeelden zijn bestanden op openbare file servers, de content in een peer-to-peer netwerk, filmpjes op Youtube, geroddel op blogs of vluchtige berichtjes op twitter.

Vertrouwelijke gegevens uit de eerste drie kwadranten nu hebben de neiging om, al dan niet gemuteerd, naar het vierde kwadrant toe te trekken. Zo worden vertrouwelijke videobeelden via Youtube verspreid, komen compromitterende foto's via sociale media als Facebook in de openbaarheid en worden bekende personen op blogs dood verklaard terwijl ze nog springlevend zijn. Er zijn zoveel voorbeelden.

Een puber filmt zichzelf in een ongebruikelijke situatie; klasgenoten zetten het filmpje op internet. Een man breekt in op de computer van een bekende presentatrice en vindt daar filmpjes; hij zet ze op internet. De beelden van een beveiligingscamera worden doorgespeeld aan de redactie van een televisieprogramma; daarna belanden ze op internet. De Spaanse politie arresteert een drugshandelaar; op internet kun je gemakkelijk vinden wie al zijn vrienden zijn.

Het is alsof informatie op internet de tweede wet van de thermodynamica volgt. Het systeem neigt naar maximale entropie, een zo groot mogelijke wanorde, een toestand waarin geen enkel gegeven meer is opgeslagen in een veilige container, maar waarin alle informatie vrijelijk in de openbare, oncontroleerbare ruimte rondzwerft. Wat geheim was, wordt openbaar; wat onder controle was, wordt onbeheersbaar, in een proces dat misschien nog het meest lijkt op diffusie. Hete informatie komt sneller in de vrije ruimte terecht dan koude informatie. En eenmaal in die ruimte is informatie slechts met de grootste moeite weer onder controle te brengen.

Wat geldt voor persoonsgegevens geldt ook voor de vertrouwelijke gegevens van bedrijven en instellingen. Organisaties hebben daarbij als nadeel dat vertrouwelijke gegevens over steeds meer bronnen verspreid zijn; niet alleen servers en mainframes, maar ook de laptops en mobiele telefoons met camera's van werknemers en onderaannemers. Tenslotte zijn ook organisaties zeer gevoelig voor de circulatie van onjuiste informatie in het vierde kwadrant, omdat de reputatie of bijvoorbeeld de beurskoers zo gemakkelijk door derden beïnvloed kunnen worden.

4. Conclusies

Langs alledrie de onderscheiden dimensies van privacy is het zeer onrustig. Het juridische fundament lijkt stabiel, maar staat onder politieke, praktische en tegenwoordig ook wetenschappelijke druk. De technologie is aan sterke verandering onderhevig en dat maakt het beschermen van persoonsgegevens steeds lastiger. De sociaal-economische dimensie tenslotte ontwikkelt zich op een onvoorspelbare manier die alleen maar lijkt te leiden tot een verdere aantasting van privacy, gewild of ongewild. Het explosieve succes van sociale media is daar een voorbeeld van. Deze combinatie van factoren leidt tot een massale en onomkeerbare verhuizing van gegevens vanuit de persoonlijke levenssfeer naar de openbare digitale ruimte. En zo lijkt het erop dat niet overheden of multinationals de grootste bedreiging voor onze privacy vormen, zoals we een kwart eeuw geleden dachten. De grootste bedreiging zijn wij zelf, geholpen door de wet van Moore.

Hoe erg is dit alles nu? Mensen van mijn generatie en ouder kunnen zich er nog druk om maken. Maar wij zijn opgegroeid in een tijd waarin het vierde kwadrant nog niet echt bestond. Komt ons ongemak voort uit onbekendheid? De volgende generatie lijkt zich minder zorgen te maken. Zij groeien op in het vierde kwadrant, gebruiken de vrije ruimte om zichzelf te profileren, om vrienden te maken, om samen te werken. Ze maken hun persoonlijke levenssfeer openbaar en vinden de hele discussie over privacy niet bijster relevant. We weten niet of dat zo blijft. We weten ook niet in welk technologisch of sociaal-economisch landschap toekomstige generaties zullen opgroeien. Maar een ding is zeker. Onze kijk op privacy zal de komende jaren ingrijpend en definitief veranderen.