Auteur: Jan Willem de Vries is jarenlang actief geweest in de wereld van informatiebeveiliging en IT-architectuur bij o.a. Capgemini. Na zijn formele pensioen was hij nog enige tijd werkzaam bij de Kamer van Koophandel als architect security. Hij is nog steeds actief als docent/trainer op beide onderwerpen. Jan Willem is bereikbaar via: janwillem.de.vries@xs4all.nl

Privacy in het dagelijks leven

Er wordt veel aandacht aan privacy besteed in de vakbladen en daarbij wordt veelal en terecht gerefereerd aan de AVG. Dit was onder meer het geval in het iB-Magazine 5 2021, waarin onder andere werd ingegaan op AVG en op de WPG. De artikelen werden geschreven vanuit de wet- en regelgeving en hadden een positieve grondhouding over wat er met de wet bereikt kan worden.

De vraag is of deze positieve conclusie terecht is. Ik had graag in hetzelfde nummer een verhandeling gezien over de werkelijke situatie met betrekking tot privacy. Is privacy-bewustzijn toegenomen en is het niveau van privacy door AVG (en WPG e.d.) zelfs verbeterd? Ik heb er mijn twijfels bij.
In dit artikel wil ik, zonder dat ik hier een wetenschappelijke studie aan heb gewijd, betogen dat het de afgelopen paar jaar slechter is gesteld met privacy in Nederland en wil ik afsluiten met een aantal voorstellen voor veranderingen. Veranderingen overigens die alleen door politieke druk (en lobbywerk) kan worden bereikt.

Bedreigingen en oorzaken

Hoe komt het dat, ondanks een privacywetgeving en ondanks goede initiatieven vanuit met name het Europees Parlement, het privacy-niveau achteruitgaat? Ik zie dat vanuit verschillende richtingen onze privacy wordt bedreigd: de overheid, de banken, sociale media, fysieke winkels, surveillance industrie en websites; en ik zal nog wel niet compleet zijn. Ik zie hiervoor een paar grote oorzaken en ik weet dat ik daarmee ook politieke uitspraken doe.
Er zijn (grote) problemen in de maatschappij – drugs, geweld, witwassen, fraude, politiek extremisme aan linker- en rechterkant – waar de overheid terecht zicht op wil hebben of krijgen. De diensten die hierop gericht zijn, lopen in hun dagelijkse praktijk aan tegen beperkingen door wet- en regelgeving. In plaats van creatiever te zijn binnen de bestaande regelgeving gaan ze er juist buiten en krijgen daarbij impliciete en expliciete steun van de overheid. Daar komt bij dat het erg lijkt dat de overheid de burgers niet als hun opdrachtgevers beschouwt, maar, al dan niet bewust, als lastige onderdanen die ze niet vertrouwen – zie ook Toeslagenschandaal en het Fraudesysteem van de Belastingdienst, alsmede de werkwijzen van UWV en bijstandsdiensten van de gemeenten. De Tweede Kamer heeft daar zelf ook zeer aan meegewerkt na de Bulgarenaffaire.

De consequentie is dan dat dezelfde overheid die gedwongen door Europa de AVG als wet heeft aangenomen, nieuwe wetten voorstelt en laat aannemen die hier tegenin gaan (Wet gegevensverwerking door samenwerkingsverbanden (WGS), Wetsvoorstel wettelijke grondslag voor verwerking persoonsgegevens (NCTV), maar waartegen vanuit privacy-organisaties, waaronder de Autoriteit Persoonsgegevens, grote bezwaren zijn.Het is een voorbeeld van een werkwijze die de Nederlandse overheid voortdurend lijkt te volgen: (beperkende) wetgeving oprekken, wetgeving voorstellen die rechtszekerheid benadeelt, processen traineren (Groningen, Toeslagenaffaire, maar ook vele zaken waarbij burgers de overheid dwongen tot correcties). Het kapitalisme tot in het extreme. De recente bankenrichtlijn PSD2 is typisch een voorbeeld van de lobby van grote IT-bedrijven die de burger een behoefte aanpraten: als wij jouw bankgegevens mogen inzien of zelfs namens jou betalingen kunnen regelen, dan… en dan komt het grootse vergezicht aan mogelijkheden. Hier zie je dat het grote geld het gewonnen heeft van de privacy van de burgers. Je kan er als burger nee tegen zeggen – en dat heb ik gedaan –, maar velen zullen en kunnen de consequenties van deze zaken niet overzien. De burger op het internet niet als klant zien, maar als

product of grondstof. Veel surveillancetechnologie die aanwezig is, is het gevolg van het feit dat sociale media, met Facebook voorop, het internet hebben kapotgemaakt ter eigener voordeel. Door gegevens te verzamelen (welke websites bezoek je, op welke advertenties reageer je, op welk deel van de webpagina blijf je wat langer hangen) en deze gegevens te aggregeren en te verrijken met gegevens van andere organisaties, kunnen ze hele profielen verkopen. Om dat mogelijk te maken, zijn er allerlei technieken in het leven geroepen om burgers te kunnen volgen, ook als ze even niet op Facebook of Twitter zitten. De overheids-surveillanceorganisaties van diverse landen maken hier ook dankbaar gebruik van. Als de Facebooks e.d. echt gericht waren geweest op bescherming van hun grondstoffen (meer zijn we immers niet) waren de systemen op onze eindstations (browsers, tablets, smartphones) veel geslotener geweest en daarmee beter beveiligd.

Dictatoriale regimes (zoals China, Rusland) willen 100% grip op hun onderdanen houden. Technologiebedrijven en wetenschappers willen graag hun kennis verkopen en werken mee aan technologieën die dit mogelijk maken: trackingsystemen, gezichtsherkenning, spraakherkenning, etc. En deze landen bieden omgekeerd dit soort diensten aan aan andere overheden in bijvoorbeeld Afrika of Azië, maar ook in Europa. Hierdoor worden wij ook nog meer gevolgd.

Als gevolg van al dit soort ontwikkelingen zijn bedrijven dit ook in de fysieke wereld gaan toepassen: gebruik maken van Bluetoothtracking, camera's in winkels, aanbieden van hotspots in winkels; allemaal bedoeld om het koopgedrag en winkelgedrag van individuele klanten te kunnen volgen en dat bij voorkeur ook te kunnen koppelen aan specifieke klanten. De daarbij ontstane profielen zijn ook weer handelswaar geworden.

Tussentijdse conclusie

Ik kom daarmee tot de volgende tussentijdse conclusie: de AVG en overige regelgeving van de EU hebben ons een goed handvat gegeven om onze privacy te beschermen, maar tegelijkertijd zijn er door dezelfde EU, door overheden en bedrijven grote en geslaagde aanvallen op onze privacy uitgevoerd, waarbij bewust de privacy van burgers is en wordt aangetast. Naar mijn mening is op dit moment die aanval groter dan wat door de AVG kan worden beschermd.

Veranderingen

Hierboven heb ik een omgeving geschetst waarin in feite de privacy van ons als burgers, ondanks veel wet- en regelgeving in Nederland, de EU, maar zeker ook de VS, wordt verkwanseld. Ik denk dat dit anders moet. Wat er moet veranderen, weet ik zo goed nog niet. Ik heb wel wat denkrichtingen, maar die zijn vast veel te simpel.

Veel kan en moet door nieuwe wet- en regelgeving op nationaal en internationaal niveau worden geregeld. Maar deze komt niet tot stand zonder actieve ondersteuning door parlement, lobbywerk vanuit privacy-organisaties, zoals de Autoriteit Persoonsgegevens of Bits of Freedom, vakbonden en een goede en vrije pers. Bij die laatste denk ik niet alleen aan de gevestigde Nederlandse pers, zoals NRC, Trouw, Vrij Nederland, maar ook aan nieuwe persdiensten, zoals The Intercept, Now This, De Correspondent e.d.

Nieuwe wet- en regelgeving zal overigens langzaam ontstaan omdat (a) het parlement door meerderheidsakkoorden erg aan het kabinet is gebonden, (b) de benodigde en actuele kennis hiervoor vaak bij parlementsleden ontbreekt, (c) er vanuit de grote IT-bedrijven en sociale media veel tegengesteld lobbywerk plaatsvindt en last but not least (d) er altijd nog de (terechte!) angst bestaat tegen terrorisme en georganiseerde en grootschalige criminaliteit en dus vanuit de opsporingsdiensten om bijzondere rechten wordt gevraagd.

Ik schreef hierboven al dat ik niet goed weet hoe we de privacy kunnen verbeteren, anders dan door goede wet- en regelgeving. Maar waar ik aan denk – en dat zal zeker tot veel al dan niet terechte kritiek leiden – is het volgende: in de AVG is al expliciet opgenomen dat er sprake moet zijn van dataminimalisatie. De (Europese en Nederlandse) wetgeving op dit punt moet nadrukkelijker worden uitgewerkt om zeker te maken dat surveillance door bedrijven en overheden, anders dan als het vanuit wet- en regelgeving wordt geëist, niet meer toegestaan is. De volgende punten zijn daar een technische uitwerking van:

Privacy by design: websites mogen per definitie niet meer volgen, alleen bij opt-in en daar mag niet elke keer om gevraagd worden. Dit moet niet alleen betrekking hebben op cookies, maar op alle manieren waarop burgers kunnen worden gevolgd, zowel client side als server side. Natuurlijk moet een website volgen; voor goede performance of om de transacties goed te laten uitvoeren. Maar ze mogen alleen volgen wat je in de eigen omgeving doet. Niet wat je verder allemaal op je werkplek doet. Ook mag dat niet gebruikt worden voor diensten op andere websites. Voorbeeld: als ik via Google wat zoek, zie ik vervolgens op diverse websites reclames over waarnaar ik zocht. Waar

Onze vrijheid wordt bedreigd door aanvallen op onze privacy.

gaat die informatie nog meer naar toe?
De consequentie van deze beperking is dat er geen tracking reclames, pixelreclames, tracking cookies, algemene trackers (anders dan om performance van systemen te meten) meer toegestaan zijn.
PII en PHI data móet in Europa worden gehost. En dat is tegenwoordig niet zo'n rare eis meer, sinds Rusland, China, Turkije, India etc. dit ook vereisen. Ook privacygevoelige data die ontstaan door het toepassen van diensten (Zoom, Teams, Discord etc.) mogen alleen worden opgeslagen in landen waarvan de EU aangeeft dat deze betrouwbaar zijn (per definitie dus niet de VS). Wellicht kunnen dit soort eisen niet algemeen worden gesteld, maar wel aan cloudproviders en aan clouddienstverleners die zich expliciet op Europa richten: data opslaan in de regio waar deze ontstaan en deze ook niet voor analyse naar elders sturen, anders dan na afdoende anonimisering.

We moeten veel meer toe naar een situatie waarin we zelf als burgereigenaar zijn en blijven van onze eigen persoonlijke gegevens en gezondheidsgegevens. Door het gebruik van een beschermde omgeving waarin deze gegevens (versleuteld) zijn opgeslagen en middelen om gericht bepaalde gegevens vrij te geven aan specifieke gebruikers, verhogen we het niveau van onze privacy.
Wetgeving moet altijd door de Eerste Kamer getoetst worden op grondrechten, grondwet en internationale verdragen. Het wordt tijd dat de Eerste Kamer hier weer de tijd voor krijgt en neemt bij nieuwe wetgeving en daarbij ook kijkt naar werkbaarheid, proportionaliteit en risico van misbruik van maatregelen. Wetten waarover momenteel veel wordt gesproken (wetgeving voor inzage van banksaldi, wet gegevensverwerking door samenwerkingsverbanden (WGS), wetsvoorstel wettelijke grondslag voor verwerking persoonsgegevens (NCTV) zijn wellicht positief bij bestrijding van zware criminaliteit, maar zijn te zwaar om alle andere redenen en zijn dan m.i. strijdig met rechtszekerheid en zullen leiden tot zelfde soort situaties als we bij de Toeslagenaffaire al hebben gezien.
Systemen (browsers, mobiele systemen) dienen veel meer dan nu het geval is, er op gericht zijn om misbruik van gegevens te onderkennen en te waarschuwen als privacygevoelige gegevens lekken of er gevolgd wordt. Cloudproviders, clouddienstverleners en bedrijven met websites zullen periodiek via verklaringen (vgl. SOC II Type 2 verklaringen) moeten kunnen aantonen dat ze de privacy van de burgers handhaven en geen profielen e.d. doorverkopen
Dit is vooralsnog een eerste aanzet. Ik ben geen expert hierin, maar wil discussie loskrijgen. Iedereen die betere ideeën heeft, is natuurlijk welkom.

Conclusie

Onze vrijheid wordt bedreigd door aanvallen op onze privacy. Aanvallen die op dit moment vanuit de overheid weliswaar niet bewust gericht zijn op vernietiging van privacy, maar wel mogelijkheden bieden om volledige controle op mensen te hebben. Ik heb zelf nog het geloof dat onze huidige Nederlandse en Europese overheden op zich geen kwaad willen. Maar de huidige stand van technologie is zodanig dat met de hedendaagse middelen dit zondermeer wel mogelijk is, mede door druk vanuit IT, sociale media en opsporingsorganisaties.
Ik denk niet dat het te laat is; we kunnen vanuit Nederland en Europa nog maatregelen gaan treffen om de bedreigingen van onze risico's te stoppen; maar dan moeten we wel nú actie gaan ondernemen door nieuwe vertrouwenwekkende maatregelen.