Cybersecurity
De leercurve van de individu

30 september 2018
mw. mr. D. Öğretici, IT-jurist

Soort artikel: opinie
Tags: digivaardigheid, cybersecurity, AVG, privacy, eskills, Maslow

Inleiding
De Algemene Verordening Gegevensbescherming (AVG) is per 25 mei 2018 in werking getreden. Rond diezelfde periode was er – naast veel aandacht voor de AVG – ook veel belangstelling voor een sociaal mediaplatform en een data-analysebedrijf. Men zou haast kunnen denken dat de berichtgeving over grote particuliere dataverzamelaars en de inwerkingtreding van beschermingsmaatregelen (de AVG) op elkaar waren afgestemd. Immers, de berichtgeving en parlementaire aandacht voor de dataverzamelaars, bracht de dode letter van de AVG tot leven.

Maar, niets is minder waar. De AVG was al geruime tijd in ontwikkeling en in andere bewoordingen (de Wet bescherming persoonsgegevens) ook reeds in ons midden. Echter, doordat het zichtbaar is geworden dat immense hoeveelheden data kunnen worden verzameld, geanalyseerd en ingezet voor diverse doeleinden, hebben de beschermingsmaatregelen van de AVG naar mijn mening een groter bereik gekregen. Men lijkt zich bewuster van het recht op privacy en verlangt van organisaties dat deze zorgvuldig omgaan met persoonsgegevens.

> *Kleine wetenswaardigheid: 600 klachten*
> Of het een 'AVG-effect' is, kan niet worden vastgesteld in verband met de afwezigheid van vergelijkbare data, maar het is interessant te weten dat de Autoriteit Persoonsgegevens (AP) op 29 juni 2018 heeft gemeld dat er 600 klachten zijn genoteerd. [1]

In dit betoog zal ik ingaan op de leercurve van de individu inzake cybersecurity. De individu heeft immers een niet te onderschatten invloed: men kan *regeren met de voet.* De mate waarin de individu vorderingen maakt in diens persoonlijke leercurve, heeft ook in organisatieverband voordelen: een individu die in privé gewend is bepaalde beveiligingsmaatregelen te treffen en/of bewust keuzes maakt en/of gewend is de juiste expertise bij zich te betrekken, zal de algehele organisatiebeveiliging – ten minste op het gebied van bewustwording – doen bevorderen.

1.0 Privacy versus gegevensbescherming
Het recht op een privéleven (privacy) en het recht om gegevens te (laten) beschermen, hebben niet eenzelfde betekenis, maar zijn losstaande elementen die elkaar kunnen versterken: het beschermen van gegevens maakt het recht op privacy (mede) mogelijk én het recht op privacy is redengevend de bescherming van persoonsgegevens aan wet- en regelgeving te onderwerpen. De AVG (Algemene verordening **gegevensbescherming)** is dan ook primair geen privacywetgeving. Al wordt het gemakshalve – ook door mijzelf – welk vaak zo genoemd, simpelweg omdat men zich dan eenvoudiger een voorstelling kan maken van de materie.

De tijd waarin we leven is echter uitermate geschikt om deze twee begrippen van elkaar te (willen) scheiden: dat een betrokkene geen bezwaar heeft diens gegevens te delen met platform X, betekent niet dat de betrokkene automatisch platformen Y en Z toestemming heeft willen geven. Daarnaast kan het voorkomen dat de betrokkene bepaalde gegevens *wel* openbaar wil hebben, maar bijvoorbeeld diens telefoonnummer *niet.*

- De AVG verplicht platform X *niet* om de gegevens voor zichzelf te houden en/of om de wensen van de betrokkene (het niet publiceren van het telefoonnummer) mogelijk te maken.
- De AVG verplicht platform X *wel* om transparant te zijn over de ontvangers van de gegevens (platformen Y en Z).
- De AVG laat echter onverlet dat de betrokkene *zelf* een platform moet kiezen dat het telefoonnummer niet publiceert. Als men het telefoonnummer bij een platform invoert dat deze gegevens openbaar zegt te maken, kan de AVG weinig betekenen: de betrokkene heeft daarin zelf een keuzemogelijkheid tussen platformen.

Het versterken/mogelijk maken van deze keuzebevoegdheid – zo is de AVG-gedachte – wordt gerealiseerd door wettelijk te eisen dat de dataverzamelaars transparant zijn over wat ze vervolgens met de data doen: publiceren ze het, sturen ze het door naar platformen Y en Z, maken ze profielen voor advertenties etc. etc. Daarnaast krijgen betrokkenen o.a. mogelijkheden dit te controleren én verzamelde data terug te vragen.

"Het *recht* op een privéleven, *verplicht* dus niet tot een privéleven."

Het *recht* op een privéleven, *verplicht* dus niet tot een privéleven. Dat is iets wat eenieder voor zichzelf moet bepalen; hetgeen de feitelijke definitie is van privacy. De betrokkene behoudt dus een hoge mate van beschikkingsrecht en keuzebevoegdheid.

2.0 De persoonlijke leercurve: bewust + bekwaam
Afhankelijk van uw eigen professie, hebt u mogelijk met enige verbazing de laatste zin van de vorige alinea

gelezen. Indien u opgeleid en/of werkzaam bent in de psychologie en/of sociologie, zijn de begrippen *beschikkingsrecht* en *keuzebevoegdheid* zeer relatief. In dit schrijven – mede gezien mijn specialisatiebeperking – ga ik voorbij aan het onderdeel *keuzebevoegdheid* in het kader van het vraagstuk: "Bestaat de *vrije wil*?"
In dit betoog beperk ik mij tot de vraag of de individu *naar redelijkheid* voldoende informatie en/of kennis heeft om het beschikkingsrecht en de keuzebevoegdheid vorm te geven. Gechargeerd gezegd: dat men een knop weet in te drukken, een mail weet te versturen, een online formulier/profiel kan invullen of een document kan opstellen, zegt immers weinig over diens kennis omtrent het inschatten van de waarde van de gegevens en de geschiktheid van het gekozen hulpmiddel (laptop, smartphone e.d.).

Ter illustratie

1. De gegevenscombinatie van een naam, achternaam en woonplaats, vertegenwoordigt op het eerste oog niet veel waarde: er is weinig risico te duchten. Dat wordt anders als deze gegevens worden ingevuld op een online website voor ziekten en de gegevens vervolgens aan een verzekeraar worden verkocht.

2. Het wordt ook anders als blijkt dat het gekozen hulpmiddel (een laptop) onvoldoende is beveiligd. Hierbij kan worden gedacht aan de situatie waarin deze gegevens – in combinatie met andere opgeslagen en gelekte gegevens – een interessante dataverzameling vormen om *persoonsgerichte spam-berichten* te versturen voor het bemachtigen van bankgegevens.

In beide voorbeelden is er AVG-technisch niets bijzonders gebeurd:

1. De website diende transparant te zijn én moest (mogelijk) uitdrukkelijke toestemming vragen.
2. Dat een betrokkene diens eigen laptop niet heeft beveiligd, geraakt in beginsel buiten het bereik van de AVG.

Met andere woorden: zowel op het gebied van datakwalificatie (wat zijn mijn gegevens waard / wat kunnen ze waar zijn in een andere context) als op het gebied van cybersecurity-kwalificatie (welke risico's zijn er en welke maatregelen vind ik passend), dient een betrokkene een bepaalde mate van bewustzijn en bekwaamheid te verwerven, alvorens deze daadwerkelijk in staat zal zijn diens beschikkingsrecht en keuzebevoegd vorm te geven.

Ter illustratie van het onderwerp keuzebevoegdheid inzake cybersecurity, zet ik in het navolgende – afgeleid van de leerfasen van Maslow – een tabel uiteen.

Cybersecurity

	Onbewust	**Bewust**
Bekwaam	Ingeval van cybersecurity vormt dit een risico: het onderdeel onbewust kan een duurzame anticipatie op ontwikkelingen belemmeren.	De ideale samenstelling om continu te blijven anticiperen op de uitdagingen van cybersecurity.
Onbekwaam	Zeer grote risico's.	Het onderdeel bewustzijn verkleint de risico's: deze betrokkene is in staat de juiste kennis/kunde bij zich te betrekken.

Toelichting
Het verwerven van kennis en informatie ten behoeve van het weloverwogen uitoefenen van een keuzebevoegdheid, zal geenszins resulteren in een 100% cybersecurity-garantie. Het resulteert in (1) kennis over de risico's, (2) kennis over de maatregelen en (3) de mogelijkheid om een afweging te maken (vaak organisatorisch, technisch, juridisch én financieel).

Door meer te leren over de techniek en uitdagingen, biedt de individu zich de mogelijkheid te ontwikkelen van *onbewust + onbekwaam* naar *bewust + bekwaam*. Al is het ook prima mogelijk dat het resulteert in *bewust + onbekwaam,* maar dan zou de bewustwording mogelijk van invloed zijn op de keuzes om *bekwame* mensen bij de beslissing te betrekken. Beide fases zullen echter tot gevolg hebben dat er – in meer of mindere mate – sprake is van keuzebevoegdheid.

3.0 Prioriteren van cybersecurity
Als men de IT-prioriteringen van de laatste 20 tot 30 jaren bekijkt, bestaat er mijns inziens een discrepantie tussen de feitelijke ontwikkelingen/prioritering en de hiervoor genoemde leerfasen. De leerfasen gaan immers uit van het bereiken van een bepaalde mate van keuzebevoegdheid en beschikkingsrecht. En in dat opzicht is er naar mijn mening nog veel winst te behalen.

Ingeval het over IT-middelen (laptops, desktops, routers etc.) gaat, is het niet aan te bevelen de risicoanalyse te beperken tot de waarde *werkt het*. Het toevoegen van andere waarden vergt echter een ontwikkeling; een ontwikkeling waar de ICT-leveranciers ook een bijdrage aan kunnen leveren.

De ICT-leveranciers hebben namelijk – over het algemeen – meer kennis. Indien zij hun informatie inzichtelijk maken ten behoeve van de keuzebevoegdheid van de betrokkene, zal de betrokkene noodzakelijkerwijs steeds meer vertrouwd raken bij het maken van keuzes.

Als bijkomend voordeel zouden de aanbieders mogelijk ook meer draagvlak creëren voor keuzes die niet primair op gebruiksgemak en/of beschikbaarheid/continuïteit zijn gericht, maar het juiste evenwicht bieden in relatie tot cybersecurity en privacy. Tegelijkertijd kan het een krimping van klanthoeveelheden tot gevolg hebben: blijkt dat men de data niet goed beveiligt of de klanten ongewenst aan allerlei profileringen en dergelijke onderwerpt, dan hoeft dat anno 2018 niet op positieve reacties te rekenen.

3.1 Verschil tussen online en offline bewustzijn

Het is uiteraard – sec vanuit technische ontwikkeling gezien – een mooi gegeven dat we in staat zijn om steeds meer eisen te stellen aan onze IT-voorzieningen én erin slagen deze steeds geavanceerder te maken. Echter, de destijds gehanteerde prioritering, had de huidige gebruiksdoeleinden niet voor ogen. De nu gekozen gebruiksdoeleinden én de daardoor groeiende digitale belangen, zouden derhalve redengevend kunnen zijn om nieuwe prioriteringen te willen hanteren.

Voor een oplossing wordt veelal naar organisaties gekeken. Dat is grotendeels terecht en verdedigbaar, maar organisaties kunnen niet alle wind uit de zeilen wegnemen.

Ter illustratie

Nagenoeg eenieder – ik ken uitzonderingen die uit veiligheidsoverwegingen andere keuzes maken – maakt gebruikt van internetbankieren. Als er op de computer een keylogger is geactiveerd, bestaat er grote kans dat risico's – bijvoorbeeld dat een onbevoegde kennis neemt van de digitale handelingen – zich verwezenlijken.

De betrokkene én de aanbieder (in casu de bank) hebben er dus een groot belang bij om zowel het onderdeel security als het onderdeel privacy in eerste instantie te waarborgen. Tegelijkertijd ontstaat hier een spanningsveld.

De verantwoordelijkheid van de bank – voor het aanbieden van een veilige applicatie (website) – is groot, maar niet onbeperkt: de bank kan niet realiseren dat de betrokkene een antivirusprogramma op de computer installeert. Dit wordt wel vanuit de algemene bankvoorwaarden als minimumeis gesteld, maar de bank kan het niet feitelijk realiseren of controleren.

Met andere woorden: de bank verlegt de verantwoordelijkheid voor de onderdelen die buiten diens feitelijke technische en juridische beheers- en beschikkingsmacht vallen.

"Om te voorkomen dat er met communicatie iets fout gaat, gaat u veilig en zorgvuldig om met communicatiemiddelen. Dit betekent bijvoorbeeld dat u uw computer of andere apparatuur zo goed mogelijk beveiligt tegen virussen, schadelijke software (malware, spyware) en ander misbruik." [2]

Banken zijn geenszins een uitzondering hierin, maar het is wel een mooi voorbeeld omdat eenieder zich een voorstelling kan maken van de *te verliezen data* (te weten: het eigen vermogen). Daarnaast is het verleggen van verantwoordelijkheden een standaard juridisch product dat in allerlei (ook niet primair IT-gerelateerde) zaken terugkomt: "Hebt u uw bankbiljetten onbewaakt op straat achtergelaten en zijn deze vervreemd, dan is de bank niet verantwoordelijk voor de schade."

Het volledig neerleggen van de verantwoordelijkheid bij de bank, is – ook na de inwerkingtreding van de AVG – een onmogelijke opgave. Voor de integratie van het AVG-gedachtegoed, is derhalve een bewustwordingsslag in cybersecurity van belang: de bank die de biljetten na uitgifte zelf op straat legt en verwacht dat de rechtmatige eigenaar deze wel komt ophalen, zou waarschijnlijk niet op veel enthousiaste klanten kunnen rekenen. Evenmin hoeft een IT-aanbieder op enthousiaste klanten te rekenen indien deze de data van klanten op straat legt.

"Het verschil is echter dat men over het algemeen in staat is (bewust of onbewust) te beoordelen dat het onbewaakt op straat achterlaten van bankbiljetten de kans op verlies vergroot."

Het verschil is echter dat men over het algemeen in staat is (bewust of onbewust) te beoordelen dat het onbewaakt op straat achterlaten van bankbiljetten de kans op verlies vergroot. Ongeacht de vraag of op dat moment een potentiële vervreemder in de buurt is, treft men de nodige maatregelen: de bankbiljetten worden uit het zicht gehaald.

Daar staat tegenover dat de 'digitale straat' wat minder zichtbaar is, evenals 'de digitale verlieskansen', de 'digitale vervreemders' en de 'digitale opbergmogelijkheden'. Sterker nog: de digitale aanbieders zijn steeds meer onzichtbaar voor de betrokkenen: *wie (welke organisatie of individu) biedt de app aan, welke maatregelen treffen ze, waarom heeft de app zoveel machtigingen van de telefoon nodig, waar worden deze gegevens opgeslagen, onder welke jurisdictie e.d.*.

Het doorlopen van de leerfasen is dus een kwestie van tijd, bereidheid en capaciteit om in meerdere maten bekwaamheid te verwerven. Daarnaast werpt het de vraag op: "Wat mag het 'plug-and-play'-principe mag *kosten*?". Is het de betrokkene de moeite waarde – zal het de moeite waard worden – een extra wachtwoord in te moeten voeren, enige kosten te moeten maken voor beveiligingsmaatregelen en/of bepaalde diensten achterwege te laten?

4.0 De belangrijke rol van organisaties
Tot dusver heb ik met name de individuele leercurve besproken. Een enkele individu heeft echter een beperkte invloed op de keuzes die ICT-leveranciers maken. Dit brengt mij tot een andere belangrijke actor: organisaties.

Organisaties hebben – in relatie tot ICT-leveranciers – veelal de wettelijke kwalificatie van verwerkingsverantwoordelijke. Hieruit vloeit de verplichting voort om met verwerkers – een doelgroep waar ICT-leveranciers ook onder kunnen vallen – afspraken te maken over technische en organisatorische beveiligingsmaatregelen.

Organisaties kunnen (/zijn bij wet verplicht) zich goed (te) laten informeren over de *passende technische en organisatorische maatregelen* die de ICT-leverancier zal treffen. Dit is een mooi aanknopingspunt om met de ICT-leverancier het gesprek aan te gaan. Ingeval de organisatie tot het oordeel komt dat de ICT-leverancier niet of onvoldoende maatregelen treft, kan dit (1) alsnog worden afgesproken of (2) zal de organisatie een andere ICT-leverancier in overweging kunnen nemen.

Deze externe invloed van organisaties is veelal het gevolg van een interne ontwikkeling inzake cybersecurity. Indien de intern verantwoordelijke medewerkers en/of adviseurs in een bepaalde leerfase zijn aanbeland, zal dit zich vertalen naar kritische vragen, gedegen advies en een groter bereik van *het cybersecurity-gedachtegoed*.

Daarentegen is de afwezigheid van een dergelijke ontwikkeling risicovol, zowel voor de organisatie zelf als voor de algehele ontwikkeling van cybersecurity. Het is daarom altijd raadzaam om te beoordelen of de gegevensbescherming van de professionals in de *daartoe bestemde* leerfase is beland.

Risicosignalen voor een nader onderzoek zijn o.a.:

> *Het zal wel goed zijn,*
> *Nagenoeg alle organisaties maken gebruik van de diensten van bedrijf X,*
> *Bedrijf X is zo groot dat ze heus voldoende maatregelen treffen,*
> *Bedrijf X is aan de AVG onderworpen,*
> *Het is heel gemakkelijk in gebruik,*
> *We zitten in de cloud (zonder toe te kunnen lichten wat voor cloud) en*
> *Adviseur Y zal het wel weten, die heeft daar immers voor geleerd.*

De bovengenoemde gedachtegang is voor een individu – die alleen diens eigen belangen heeft de beschermen – tot op zekere hoogte houdbaar. Ingeval een organisatie of de daar werkzame professionals zich van dergelijke argumentatie bedienen, is nader onderzoek ten zeerste aan te bevelen.

5.0 Slotwoord
In betoog heb ik vanuit mijn professie als IT-jurist getracht enige gedachten uiteen te zetten over cybersecurity, de AVG en de invloed van individuen.

De AVG is geenszins het eindstation voor wat betreft de uitdagingen van cybersecurity. Het is eerder een beginstation, omdat de AVG voor meerdere organisaties en individuen redengevend is geweest een verdieping te zoeken in privacy en cybersecurity. Niettemin is er nog veel ruimte voor ontwikkeling, waar de algehele toename van kennis en kunde een bijdrage aan zal leveren.

Om hier enige houvast in te bieden, heb ik een overzicht van leerfasen – afgeleid uit de leerfasen van Maslow – uiteengezet. Individuen en organisaties doen er mijns inziens goed aan om voor zichzelf en de bevoegde professionals te bepalen in welke leerfasen zij zich bevinden. Immers, het duiden van de leerfase, zal van wezenlijk belang zijn op de mate waarin *bewustwording* en de *acceptatie van maatregelen* zal toenemen.

Een – *naar de stand van de techniek* – goede cybersecurity gaat niet in alle gevallen voorbij aan het gebruiksgemak. Er zijn inmiddels meerdere ICT-leveranciers die cybersecurity én gebruiksgemak in juiste verhouding weten aan te bieden. Het blijft echter een *menselijke* afweging deze diensten wel of niet in gebruik te nemen. Daartoe dient een bepaalde *intrinsieke motivatie* aanwezig te zijn, welke mijns inziens wordt versterkt door de leerfase waarin men zich bevindt. Daarnaast zal de leerfase in de gevallen er wel enige concessies op gebruiksgemak worden gedaan, voor een hogere mate van acceptatie en/of risicobeoordeling zorgen.

Volgende publicaties
Als vervolg op dit artikel, ben ik reeds in conceptvorm artikelen aan het schrijven over:

(1) De piramide van cybersecurity
Een artikel waarin de basisvereisten van IT-middelen stapsgewijs worden toegelicht.

(2) Verzekeren van groeiende digitale belangen
Een artikel waarin de effecten van digitale verzekeringen op cybersecurity worden toegelicht. Immers, een verzekeraar zal ook minimale eisen stellen, alvorens een verzekering kan worden afgesloten.

(3) Praktische tips voor individuen en organisaties
Een artikel waarin uiteen wordt gezet wat layered security is en welke *cybersecurity-vraagstukken* van belang zijn voor een goed informatiebeveiligingsbeleid.

Wilt u aan deze artikelen meewerken en/of van gedachten wisselen?
Een samenwerking met stel ik uitermate op prijs. U kunt uw interesse kenbaar maken via privacy@exlege.nl.

Wilt u meer weten?
Neem vrijblijvend contact op voor meer informatie.

Bronnen
1. Autoriteit Persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ruim-600-mensen-dienen-privacyklacht-bij-ap, laatst geraadpleegd 4 september 2018.
2. Artikel 16 algemene bankvoorwaarden 2017 (Nederlandse Vereniging van Banken), https://www.nvb.nl/publicaties/protocollen-regelingen-richtlijnen/1173/algemene-bankvoorwaarden-abv.html, laatst geraadpleegd 4 september 2018.