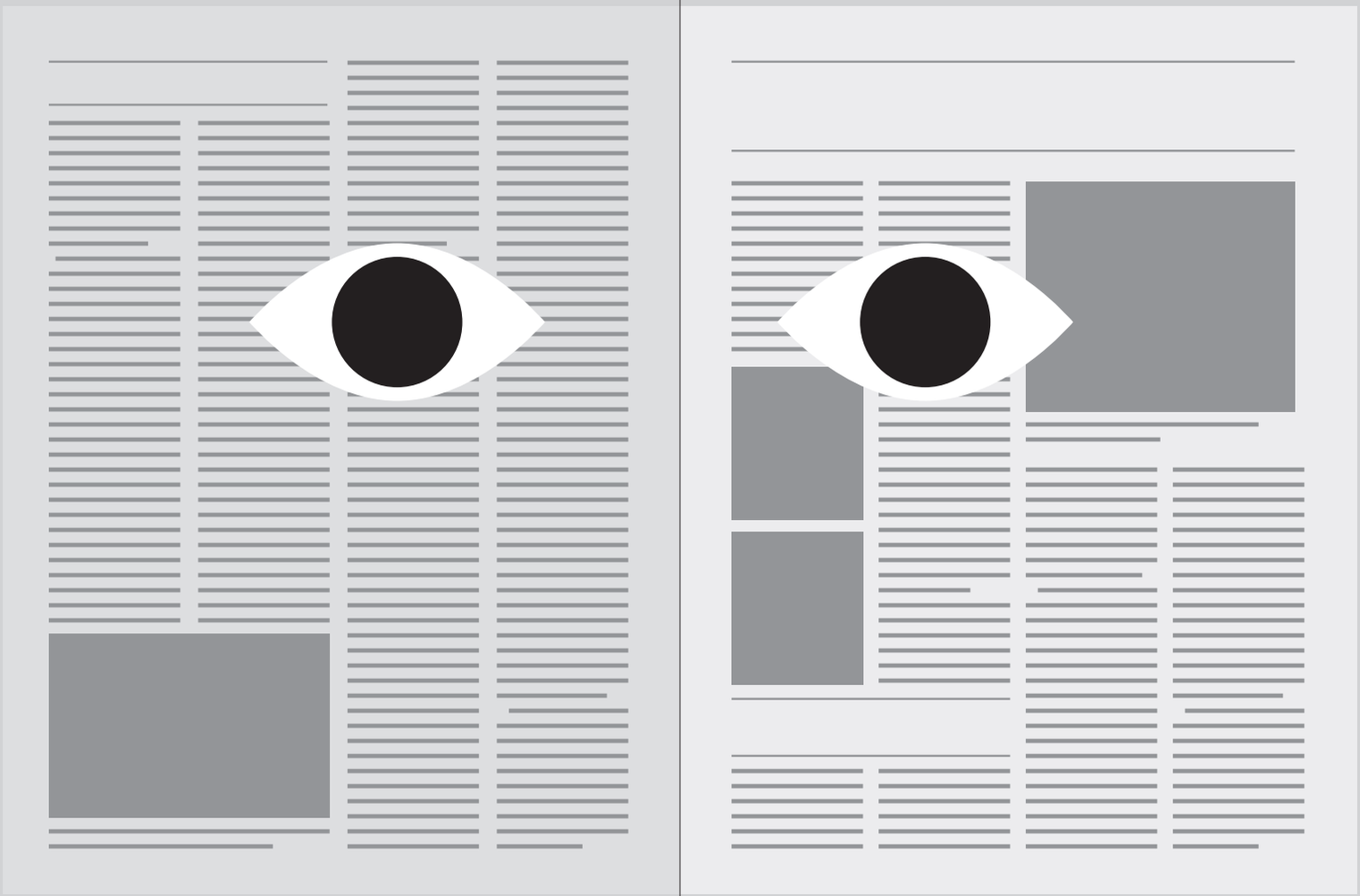
Hoofdstuk 2.
Privacy actueel



Onze privacy staat onder druk, dat is geen geheim meer. Politici van elke strekking gebruiken hun ideologie om onze privacy beetje bij beetje te verminderen, soms bewust, soms onbewust. Afhankelijk van het rechts-linksverhaal zijn er andere gebieden waar privacy als een wisselmunt wordt opgeofferd voor het grotere doel. Dat kan veiligheid zijn, het milieu (denk aan de knips of LEZ in vele steden) of onze gezondheid.

Niet alleen politici knabbelen aan ons privéleven. Commerciële actoren gebruiken data om ons koopgedrag in kaart te brengen. Ze stellen een psychologisch profiel op, waarbij interesses, relaties, seksuele voorkeuren, impulsiviteit en vele andere factoren nauwgezet worden bijgehouden. Algoritmes proberen vervolgens de meest relevante producten via sociale media aan je voor te stellen. Dataverzameling rendeert. Is vrije wil een illusie?

ONZE VEILIGHEID

Veiligheid heeft ons denken de laatste jaren absoluut gedomineerd. Hoewel we in principe al eeuwen te kampen hebben met oorlogen, terrorisme en onveilige buurten, dragen de grote visibiliteit op sociale media en de honger van klassieke media bij tot een dicht-bij-je-huisgevoel van terrorisme en onveiligheid.

De echte kentering kwam er door de aanslagen in de VS. Na 9/11 was niets meer hetzelfde. Niet alleen Amerikanen werden ruw weggerukt uit een naïeve veilige bubbel, iederéén zag de beelden verschijnen op tv. Vraag aan Belgen waar ze waren toen de aanslagen plaatsvonden, en de meesten zullen een vrij precies kader kunnen schetsen. De beelden staan op het netvlies gegrift.

Wanneer soldaten sterven op het slagveld, kraait er geen haan naar. Dat past immers perfect binnen ons verwachtingspatroon. Soldaten trekken naar het slagveld, soldaten vechten, soldaten sterven. Er zijn wel wat protesten, wat marsen, wat vredesactivisten, maar alles lijkt peis en vree.

Wanneer onschuldige burgers het moeten ontgelden door daden van terrorisme, breekt de hel los. Terroristen zijn in de eerste plaats doorgewinterde marketeers. In aantallen verbleekt hun schade vaak bij de vele slachtoffers in 'echte oorlogen', maar de media krijgen niet genoeg van civiele terroristische aanslagen.

9/11 bracht een golf van overheidssurveillance over de Verenigde Staten, vaak openlijk gesteund door politici en een groot deel van de bevolking. Plots voelde iedereen zich onveilig, en keek het anders zo onafhankelijke *freedom*-land naar een sterke overheid om de problemen op te lossen.

Het Edward Snowden-schandaal was een uitwas van die periode. Privacy en burgerrechten moesten massaal en zonder pardon wijken voor een totalitaire massasurveillance. Elke burger werd afgeluisterd, zowel met computeralgoritmes (spraakherkenning) als manueel. Jaren later blijkt massasurveillance weinig tot geen resultaten te hebben opgeleverd. Alle terroristen die werden opgespoord, waren het resultaat van gerichte surveillance, en van onderzoekswerk. Zoals het hoort.

Het was te laat. Na Snowden kregen projecten een nieuw naam, ze werden opgeschoond, en de NSA en andere veiligheidsdiensten deden gewoon verder.

Ook in België bleven we niet gespaard van de terroristische dreiging. In 2016 vielen er 32 levens te betreuren bij zinloze aanvallen in Zaventem en Brussel. Eigenlijk 35, maar de drie terroristen die om het leven kwamen, wel, daar treurt niemand om. Een golf van paniek en angst waarde door het land. Het veiligheidsniveau — dat al jaren vast lijkt te liggen op niveau 3, het op een na hoogste — werd prompt op 4 geplaatst. Drie dagen nationale rouw. Evacuaties. Reportage na reportage na reportage. Beelden, op het netvlies gebrand, van bebloede mensen die de vertrekhal van de luchthaven uit zigzaggen. Het zijn beelden die we nooit meer vergeten.

En toch. In 2018 werden er 38.455 verkeersongevallen geteld met in totaal 49.354 slachtoffers: 45.114 lichtgewonden, 3.636 zwaargewonden en 604 personen die om het leven kwamen binnen dertig dagen na het ongeval. Het doet geen stof opwaaien. Om de zoveel dagen is er een klein artikeltje over een dodelijk ongeval, het is geen nieuws. Het maakt ons niet bang, want het verkeer op de Belgische wegen neemt elke dag toe.

Het is altijd lastig om absolute cijfers naast elkaar te leggen, wanneer emoties de overhand nemen. Mensen — en politici zijn voorlopig nog steeds mensen, al gedragen ze zich er misschien niet altijd naar — zijn inherent emotionele wezens. Het heeft geen zin om absolute cijfers of grafieken te gebruiken om het onveiligheidsgevoel te meten.

Wat wel zin heeft, is het wettelijk optreden evalueren. Na de terroristische aanslagen in 2016 nam het federaal parlement twee antiterreurwetten aan (de zogenoemde Terro II- en Terro III-wet). Ook de bijzondere inlichtingen- en opsporingsmethoden kregen een opknapbeurt. Verder werd een nationaal noodplan uitgewerkt in een Koninklijk Besluit en vonden heel wat 'ondenkbare' maatregelen plots zonder enige tegenspraak doorgang.

Een daarvan draait rond dat kleine kaartje in je smartphone: de simkaart. Nu al zo klein als een vingernagel (de nano-sim), stelt deze technologie ons in staat om een nummer te koppelen aan een toestel, en dus om oproepen te ontvangen en op het mobiel internet van de operator te surfen. Verder is het niet zo'n enorm intelligent kaartje, maar daar draait het debat hier niet om: vroeger kon je zo'n kaartje anoniem kopen. Nu kan dat niet meer.

Ik ben oud genoeg om me te herinneren hoe makkelijk het was om een prepaid nummer te gaan kopen in een dagbladhandel of vakwinkel. Je stak dat in je gsm, zette er wat geld op en hop, je kon naar believen sms'en. De goede oude Nokia — die privacyactivisten soms met de nodige weemoed doet terugdenken aan de tijd waarin men zich redelijk anoniem kon bewegen in het leven.

De Belgische terroristen ontnamen de Belgische bevolking die belangrijke mate van anonimiteit. Elk telefoonnummer is nu gekoppeld aan een identiteit, via je identiteitskaart en rijksregisternummer.

Herhaaldelijk vroeg ik de toenmalige bevoegde minister Alexander De Croo om uitleg. Diezelfde minister had immers luttele maanden voor de aanslagen laten optekenen dat hij anonieme simkaarten nooit zou afschaffen, omdat niet elke burger een crimineel is. Dat terrorisme een wending kan geven aan idealen, kan men nog begrijpen. Dat er echter nooit een antwoord kwam op de vraag hoe deze maatregel zou helpen in de strijd tegen terrorisme, zet aan tot denken — en toegegeven, de nodige frustraties.

Terroristen walsen immers niet zomaar een telecomwinkel binnen, op zoek naar een simkaart. Die bestellen ze nu gewoon in het buitenland, in landen waar de identificatieplicht niet geldt (en wellicht nooit zal gelden). Of ze gebruiken helemaal geen simkaart of een die gestolen werd. Vervolgens sturen ze niet zomaar sms'jes naar elkaar: 'Morgen gerechtsgebouw Gent opblazen. 13u. Be there.' Ze gebruiken applicaties zoals Telegram en Signal, die encryptie en anonimiteit waarborgen. Ze gebruiken codetaal.

De enigen die de overheid met zo'n maatregel raakt, je raadt het al, zijn onschuldige brave burgers die zich graag wat anoniemer zouden willen bewegen. Een smartphone is immers zoveel meer dan een telefoon: het is een afdruk van je persoonlijkheid. De locaties die je bezoekt (die via de simkaart af te lezen zijn, via de zendmasten) verraden je woonplaats, werk, hobby's en zelfs intieme geheimen.

De teloorgang van de anonieme simkaart is een illustratie van een reeks maatregelen die werden genomen in het kader van de 'showbizzpolitiek'. Politiek moet men de laatste jaren vooral zíén doen, en dat het liefst op Twitter of andere ongenuanceerde platformen. De echte waarde van beslissingen verdwijnt naar de achtergrond, de debatten worden gevoerd in achterkamers, het parlementair debat verbleekt bij de straffe taal van enkele politici.

Terroristische aanslagen zijn hét gedroomde instrument om de bevolking op te zadelen met beslissingen en maatregelen die er anders nooit of te nimmer zouden doorkomen. Het is in momenten van crisis, in momenten van diepe rouw, in momenten van blinde paniek, dat de aandacht voor de rechten en vrijheden van individuele burgers zodanig

verslapt dat men de kans schoon ziet om allerhande onnodige en bijwijlen gevaarlijke regels in te voeren.

Terroristen zijn ook electoraal goud. Hoe onveiliger Jan Modaal zich voelt, hoe meer die een sterke overheid wil. En een sterke overheid, dat is een overheid die over bijzondere macht en budget beschikt. Het onveiligheidsgevoel — waar in binnen- en buitenland heel wat partijen op teren — creëert ook een wij-zij-scenario, op zich een eeuwenoud recept om mensen binnen een bepaalde groep dichter bij elkaar te brengen en de onderlinge verschillen uit de vlakken.

Dat gold ooit voor de slaven in Rome, de Spartanen in Griekenland, de heidenen in de middeleeuwen en, recenter, de Joden in Europa. Nu is het een andere religie die het moet ontgelden, maar dit boek draait niet om rassenhaat.

De slogan waarmee de N-VA naar de verkiezingen trok was 'Veilig thuis in welvarend Vlaanderen'. Veiligheid was een gedroomde pijler voor de rechtsconservatieve partij, die de emotie van de gemiddelde Vlaming toch redelijk goed kon peilen de laatste jaren — al verloor de partij gevoelig aan Vlaams Belang.

Die rush naar een veilig Vlaanderen bracht een zondvloed van slimme en domme camera's, identiteitskaarten met vingerafdrukken, afluisterapparatuur en ander fraais met zich mee. De kostprijs en wetenschap waren irrelevant: of het werkte of niet, het móést gedaan worden.

Het zou overigens bijzonder oneerlijk zijn om enkel naar de N-VA te wijzen. Lokale koplopers in cameragebruik, soms met afluisterapparatuur en slimme technologie, zijn Mechelen en Kortrijk, waar liberale kopstukken de plak zwaaien. Zowel Bart Somers als Vincent Van Quickenborne (Open Vld) tonen zich ongebreidelde liefhebbers van ingrijpende surveillancetechnologie. Zo staan er nergens meer slimme camera's dan in Mechelen en werkt Van Quickenborne al jaren samen met operator Proximus om 'mensen te tellen'. Waarvoor dat dan weer goed is, geen idee. Citymarketing heet zoiets, en het klinkt even onnozel als het ook echt is.

Ook aan groene zijde is er weinig reden tot optimisme. De groenen — behept met een zeker streven om de 'wereld te verbeteren' — willen absoluut Koning Auto onttronen. Creatieve knips, andermaal uitgerust met slimme camera's, moeten de binnenstad ontlasten, met gekreun van de stadsring tot gevolg. En niet te vergeten de LEZ, de veelbesproken lage-emissiezone die oude diesels moet weren, waarbij speciale camera's als moderne tolpoorten aan de invalswegen van steden worden geplaatst.

De camera's zoemen zeven dagen op zeven, vierentwintig uur op vierentwintig. Ze volgen elke verplaatsing, bespieden ons vanuit een grote schimmige controlekamer. De boetes volgen automatisch. We praten weleens laatdunkend over China, maar zo heel ver staan we er niet meer vanaf.

Wat dit politiek relaas vooral bewijst, is dat men onze privacy stilaan beschouwt als een vervelende wisselmunt zonder veel waarde, die moet wijken voor ideologie en dromen. De een droomt van veilige straten, de ander van propere. De burger — die keer op keer hoort dat hij een 'stukje' van zijn privacy moet opgeven — loopt steeds meer het reele risico dat eens de stukjes zijn verzameld, hij wakker wordt in een wereld weliswaar vol leuke ideologieën, maar zonder enige privacy.

ANPR-camera's

Vlaanderen staat ondertussen vol met ANPR-camera's (*Automatic Number Plate Recognition)*. Er zijn weinig regio's in de EU te bedenken met zoveel slimme camera's per inwoner. Die ANPR-camera's hangen er tegen terroristen: dat was de leuze en het opzet. Gevaarlijke criminelen mochten niet langer door de mazen van het wegennet glippen en deze camera's — hoewel ze iedereen voltijds volgen, dus ook alle onschuldige burgers — moesten zorgen voor een daadkrachtig politieoptreden.

De realiteit is, zoals met zovele zaken, toch gevoelig anders. De overgrote meerderheid van ANPR-meldingen (zoals onverzekerde wagens, geseinde nummerplaten...) verdwijnt namelijk in het sepot. Politiediensten en -zones hebben simpelweg de mankracht niet om de

dure spulletjes van verkozen burgemeesters en politici ook daadwerkelijk nuttig in te zetten.

De enige partij die écht profiteert van deze cameragekte, is degene die ze mag verkopen (en plaatsen). Dat is een consortium van twee bedrijven: Proximus — allang geen simpele telefoonoperator meer — en Trafiroad, het bedrijf van Glenn Janssens. Zij verdienen miljoenen aan overheidscontracten, want ze zijn de enige partij in Vlaanderen die gemachtigd is om ANPR-camera's neer te planten.

De ANPR-camera's liggen om meerdere redenen gevoelig. Er is — in volle besparingsperiode, waarin sectoren op alle mogelijke manieren moeten bezuinigen — eerst en vooral het kostenplaatje. Het nationaal cameraschild moet oplopen tot drieduizend camera's, duizend ervan staan er al. Dat komt bovenop de initiële investering van 36,5 miljoen euro in de duizend camera's, het centrale systeem dat elk jaar 2,5 miljoen euro kost aan onderhoud en de huur van de lijnen, én 10 miljoen euro voor tweehonderd voltijdse personeelsleden om de geregistreerde gegevens te behandelen.

Met Trafiroad gaat het goed. Het bedrijf verkoopt en verhuurt wegsignalisatie, en zelfs kerstverlichting, en floreert nu vooral op camera's en elektronische surveillance. De omzet loopt in de vele tientallen miljoenen. Er is dus grof geld mee gemoeid, en zoals altijd: *follow the money*.

Die *money* komt echter van jou en mij: de camera's worden uiteraard gezet met belastinggeld. Aangezien er maar één speler kan bieden, is de prijs onnatuurlijk hoog voor het geleverde product en de bijbehorende dienst. Geen haan die daarnaar kraait, want deze private lobbymachine draait overuren bij politici.

Naast het wereldlijke financiële aspect, is er uiteraard nog een rist ethische en juridische bezwaren te ontrafelen. Hoe ethisch vinden we het dat we geen enkele verplaatsing meer kunnen maken zonder dat de overheid daarvan weet? De beelden staan immers dertig dagen ter beschikking van de lokale overheid, maar tot liefst een jaar van de federale overheid. Ook de geheime dienst krijgt toegang tot alle beelden. Zoals ook de praktijk dagelijks bewijst, is de politie niet gebaat bij een

overschot aan beelden: een crimineel zoeken is meestal een naald in een hooiberg, en dat wetende maakt men gewoonlijk de hooiberg kleiner, niet massaal groter.

In dit geval is de toestroom van beelden gigantisch groot, aangezien men elke onschuldige burger filmt. Alles in de filosofie van *predictive policing*: het is niet omdat je op dit moment onschuldig bent, dat dat binnen enkele weken of maanden nog steeds het geval is. De ANPR-camera's zouden echter zoveel nuttiger zijn, mochten énkel geseinde criminelen (en hun nummerplaten) actief worden gefilmd, terwijl onschuldige nummerplaten en burgers meteen gewist worden. Zo kan men de privacyinbreuk proportioneel maken: enkel de bewegingsvrijheid van criminelen wordt ingeperkt. Dat maakt het systeem zoveel nuttiger voor de politie, en het is eerlijker.

Het is onbegrijpelijk dat deze vraag niet breed wordt gesteld door de verantwoordelijke politici, laat staan dat deze piste ernstig wordt onderzocht. Het is niet overdreven om te wensen dat je je op de openbare weg kan verplaatsen zonder dat de overheid hier telkens van op de hoogte is. Zelf zie ik liever een wereld zonder camera's, maar ik heb voldoende realiteitszin om te beseffen dat dit stilaan een quasi onmogelijke eis wordt.

Sommigen beweren dat men geen privacy meer heeft eens men zich in de publieke ruimte zou bevinden. Anders gesteld: privacy is er enkel binnen de vier muren van je huis. Dat klopt natuurlijk niet, ook in het publieke domein is en blijft privacy belangrijk, al zijn de mate daarvan en de verwachtingen daarrond uiteraard verschillend.

De gruwelijke moord op Julie Van Espen wordt veelvuldig ingeroepen door mensen die fan zijn van camera's. Maar wordt het leed van haar familie en vrienden hier niet simpelweg misbruikt? De moordenaar van Julie werd immers niet gevonden door een *slimme* (of ANPR-)camera, maar wel door een *domme* private bewakingscamera van een bedrijf. Daar dienen camera's ook gewoon voor: als (en enkel als) er een misdrijf plaatsvindt, kan men gaan kijken naar de beelden. Ik ken maar weinig privacyvoorvechters die zich daartegen zouden verzetten. Ten tweede: camera's stoppen géén misdrijven. Dat is belangrijk om te onderstrepen,

want blijkbaar sijpelt dat besef niet steeds door. Camera's vervullen een soort voyeuristische nood, maar grijpen niet in waar een politieagent of waakzame burger dat wel kan en moet doen. Bovendien was de moordenaar van Julie een wel erg domme crimineel: had de man een petje of bivakmuts opgehad, dan waren alle dure camera's volledig nutteloos.

Ik pik er Julie Van Espen uit omdat zij bijna dezelfde emotionele nationale waarde heeft gekregen in onze media als de terroristische aanslagen. Er gebeuren immers dagelijks vreselijke misdaden. Maar als men dan toch het jonge leven van deze vrouw, en deze volkomen zinloze en gruwelijke daad, politiek wil gebruiken, laat het dan tenminste op basis van juiste argumenten zijn, niet op basis van foute populistische informatie.

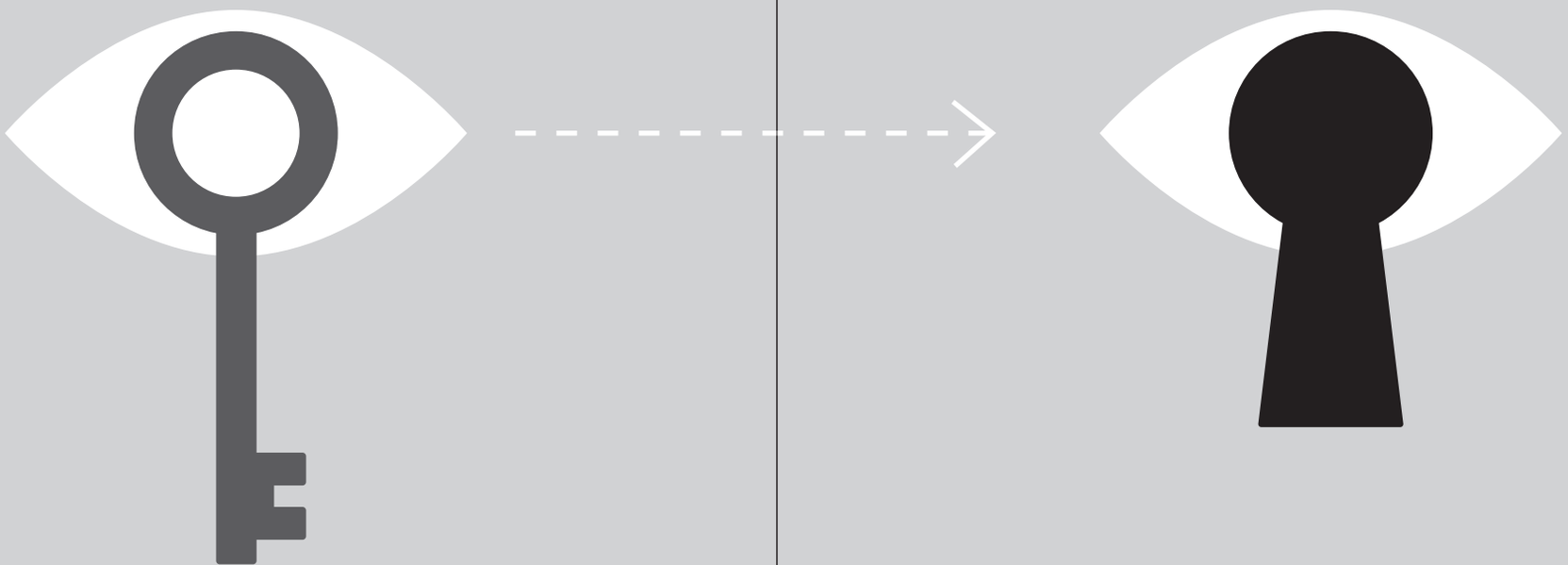
Feit blijft dat deze camera's ook weer vooral onschuldige brave burgers raken. Misschien niet direct (je auto ontploft niet wanneer hij een camera passeert), maar zeker wel indirect en de gevolgen zijn niet altijd even zichtbaar. De maatregelen die men nam tijdens de lockdown in 2020 bewijzen dat de gevolgen niet altijd veraf zijn: plots werden de ANPR-camera's gebruikt om inwoners en bezoekers te volgen en op automatische basis GAS-boetes uit te schrijven voor 'niet-essentiële verplaatsingen'. Het systeem dat er zogezegd enkel stond voor terroristen en zware criminelen, werd nu opeens gebruikt tegen Piet en Els die een paar kilometer te ver van hun woonst boodschappen gingen doen.

Vingerafdrukken

De saga van de vingerafdrukken begint ergens in 2015. Jan Jambon (N-VA) kwam terug van staatsbezoek in Marokko en was overdonderd door de biometrische beveiliging die de Marokkaanse overheid introduceerde. De identiteitskaarten van Marokkanen bevatten immers niet alleen vingerafdrukken, maar ook nog andere biometrische data. De Marokkaanse *smart card* wordt beschouwd als een van de meest verregaande identiteitskaarten ter wereld.

Jambon keerde euforisch terug naar België en liet optekenen dat hij een dergelijke identiteitskaart ook wou onderzoeken voor Belgische

Hoofdstuk 3.
Privacy praktisch



Wat is een boek zonder praktische houvast? Wat heb je als lezer aan een academische beschrijving van het begrip privacy, of een verhaal vol doemdenken? We geven je in dit hoofdstuk een praktische inkijk in tal van sectoren waar je privacy onder druk staat, en vertellen je vooral wat jij kan doen om je privéleven veilig te stellen.

Want vergis je niet: je privacy staat onder druk. Bij het shoppen, wanneer je een vliegtuig neemt, op straat, bij het invullen van je belastingen, tijdens het swipen op Tinder... Het is mijn grootste hoop dat je hieruit iets écht praktisch kan overnemen en zo je privacy beetje bij beetje kan herwinnen.

PRIVACY BIJ JE THUIS

Waar we wonen, daar zijn we veilig. Binnen de hoge muren van onze woning of ons appartement kan je eindelijk jezelf zijn. Vrij van surveillance, spiedende ogen en opdringerige verkopers. Een soort privacyoase. Maar is dat wel zo? Is onze woning nog steeds de heilige graal van onze privacy? Ja, maar toch helaas ook: neen.

Nemen we een gemiddeld gezin van vier. Vader, moeder en twee kinderen — beetje conservatief, maar goed. We gaan ervan uit dat je woning is uitgerust met een aantal comforten, schijnbaar onmisbaar in deze tijden. Internet stroomt binnen en de keuze van operatoren is daarbij beperkt: zo zal je hoogstwaarschijnlijk via Telenet of Proximus surfen. Maak je daarbij geen illusies: ook kleinere operatoren zoals Scarlet behoren gewoon tot de Proximus-groep. Enfin, er zijn nog illustere kleinere operatoren zoals EDPNet of Dommel, maar de kans dat je nog nooit van hen hebt gehoord is reëel.

Naast het internet — en zeker met een stel pubers in huis — beschik je waarschijnlijk ook over een Playstation of andere gameconsole, een *smart speaker* zoals Google Home of Amazon Alexa, een paar goedkope IP-camera's van Chinese makelij, een slimme deurbel, een aantal computers, een verloren geraakte tablet en wat smartphones. Meteen een pak minder idyllisch, die heilige graal van ons.

Tenzij je beschikt over een gezonde doses IT-kennis — en volgens sommigen een ongezonde dosis paranoia — heb je vermoedelijk weinig of niets gedaan om deze zaken dicht te timmeren. Er is één lichtpuntje: de meeste moderne routers van telecomoperatoren komen met een vrij sterk WPA2-wachtwoord, bestaande uit een reeks letters en cijfers met hier en daar een hoofdletter of een speciaal karakter. Niet waterdicht, maar alleszins al een pak beter dan het WEP-wachtwoord van een aantal jaar geleden. Met behulp van oersimpele programmaatjes kon iemand een WEP-sleutel binnen de drie minuten kraken, en daarvoor hoefde je echt geen doorgewinterde hacker te zijn. Toch veranderen nog steeds heel wat mensen hun WPA2-wachtwoord naar een makkelijk wachtwoord — lees: een woord dat in een woordenboek staat, en te kort is.

HOE MAAK JE EEN STERK WACHTWOORD?

We weten het allemaal: tenzij je een half genie bent, is het onthouden van een tiental unieke wachtwoorden een pijnlijke zaak. Zelf stond ik ooit met een black-out aan een pompstation, ik kende de viercijferige pincode van mijn bankkaart niet meer. De auteur is geen genie.

Een sterk wachtwoord maken is makkelijker dan je denkt. Maar allereerst is het van cruciaal belang dat je níét hetzelfde wachtwoord gebruikt voor verschillende websites, diensten of sociale netwerken. Hoe doe je dit, zonder om de vijf minuten te vloeken omdat je je wachtwoord niet meer weet? Simpel: door een wachtwoord*zin* te gebruiken. *Datis33nBlauwePullover* gebruik je bijvoorbeeld voor Facebook. De kleur blauw koppel je aan de stijl van het thema. Door het gebruik van hoofdletters en cijfers maak je je wachtwoordzin zo goed als onkraakbaar. Hoe meer karakters een wachtwoord telt, hoe moeilijker het voor (weliswaar simpele) software is om het te kraken. Wachtwoorden van vier of vijf karakters zijn gewoonlijk in enkele minuten gekraakt.

Je kan de kleur vervangen voor andere websites. Zo krijgt Twitter het wachtwoord *Datis33nHemelsblauwePullover.* Of je werkt met een voorvoegsel per website: *Datis33nFrissePullover* voor Twitter, *BlauwePullover* voor Facebook, *LolligePullover* voor LinkedIn, *ZaligePullover* voor Zalando, *AaibarePullover* voor Amazon… Je snapt het onderhand wel.

Of: gebruik een digitale paswoordmanager, zoals LastPass. Die houdt voor jou netjes unieke wachtwoorden bij en vult deze soms zelfs automatisch in op websites. Zet je wachtwoorden níét in een schriftje of op een blad papier (*busted?*)! En gebruik nooit of te nimmer deze top 10 van meest populaire wachtwoorden:

123456
qwerty
123456789
welkom
12345
password
welkom01
wachtwoord
1234
12345678

Ook *not done*: de naam van je lief, huisdier of kind of geboortedata.

Nog een laatste tip: gebruik 2FA (of *two-factor authentification*). Klinkt ingewikkeld, is het niet: na het inloggen met je e-mailadres en wachtwoord, krijg je een scherm te zien waar je een unieke numerieke code moet invullen, die elke dertig seconden wijzigt. Met een applicatie als Authy wordt dit kinderspel. Sterk aangeraden, want zelfs al kraakt een hacker je wachtwoord, dan kan die nog altijd niets aanrichten!

Hoe sterk je internetwachtwoord ook is, veilig ben je nooit. Het gevaar komt immers niet meteen van je nieuwsgierige buurman — die beschikt ondertussen ook zelf wel over internet — maar eerder van je leverancier. Je leest het goed: het gevaar komt uit Telenet- of Proximus-hoek!

Je operator volgt immers gewoon netjes alles mee wat je uitspookt op het wereldwijde web — en dat is amper bekend. Natuurlijk lopen onze operatoren er niet mee te koop. Stel je maar een advertentie voor waarin staat: 'Telenet-pack voor 45 euro, en wij kijken lekker mee!' Ik vermoed dat de verkoop geen grandioos succes zou zijn.

En toch is het precies dat wat er gebeurt. Onder de — ondertussen wel in oktober 2020 vernietigde — dataretentiewetgeving worden operatoren verplicht om gegevens (je identiteit en je trafiek) van je bij te houden. Vanuit Europees niveau heeft men het initiatief genomen om een regelgeving uit te werken inzake dataretentie. Dit resulteerde in de dataretentierichtlijn.

Die dataretentiewetgeving is al een aantal keer succesvol aangevochten bij onze rechtbanken, maar operatoren gaan ondertussen lustig verder met deze praktijk. In 2015 werd de Belgische omzetting van de richtlijn nog ongrondwettelijk verklaard door het Grondwettelijk Hof, maar in 2016 had België al een zo goed als identieke wet klaar ter vervanging. Die 2.0 wetgeving verschilt amper en baart privacyactivisten nog steeds grote zorgen. Fijn nieuws: in oktober 2020 werd ook de nieuwste versie ongrondwettelijk verklaard. De kersverse minister van Justitie moet dus aan de slag en een betere wet uitwerken.

De huidige dataretentie gaat dan ook ver: gedurende één jaar moeten operatoren quasi alles over jouw gedrag bijhouden. Naar wie je belt op Skype, naar welke websites je surft, hoeveel mails je verstuurt en ga zo maar door. Hoe fix je dit? Moeilijk, maar niet onmogelijk: door een tunnel te creëren tussen je internetprovider en je internetgebruiker. Vergelijk het met de Kennedytunnel: waar de autostrade het internet is dat je provider aanbiedt, is Antwerpen je eigen internetgebruik, en de tunnel, wel, dat is de VPN.

Een VPN, of *Virtual Private Network*, was al populair bij thuiswerkers van grote bedrijven, die via een VPN moesten inloggen op het bedrijfsnetwerk. De laatste jaren kwamen er echter meer en meer 'privacy-VPN's' op de markt, de een al wat beter dan de andere. Zo zijn er gratis en betaalde varianten — maar de gratis diensten vermijd je liever.

Praktisch zijn er twee manieren waarop je je tunnel kan creëren: of je installeert de tunnel op routerniveau, of je installeert het op elk toestel apart via een applicatie. In de eerste versie steek je dus een hardwarebakje tussen je Telenet- of Proximus-router, die dan fungeert als beveiligd netwerk. In de tweede versie installeer je een VPN-app, zoals ExpressVPN, Surfshark of NordVPN (er zijn er nog veel, veel meer). Kijk goed na welke garanties de VPN's je bieden (of ze bijvoorbeeld een externe audit ondergingen of niet), hoeveel je betaalt voor een of meerjarenabonnement, enzoverder.

Terug naar onze Kennedytunnel. Wie daar geregeld passeert, zal vast merken dat de snelheid danig teruggeschroefd wordt. Op de autostrade rij je zo'n 120 km/u, in de Kennedytunnel (geholpen door alweer — *zucht* — een trajectcontrole met ANPR-camera's) 50 km/u. Zo drastisch is het meestal niet met een VPN, maar hou er rekening mee dat je internetsnelheid zal afnemen. Dat is logisch: je internet moet een extra baantje trekken.

Een ander belangrijk aandachtspunt is dat weliswaar Proximus of Telenet je internetverkeer niet langer ziet — het is een geëncrypteerd boeltje geworden, dus zij zien enkel onbegrijpbare code — maar je VPN-aanbieder kan je internetverkeer wel degelijk nog inkijken. Bijna elke VPN-aanbieder belooft een 'no-log' werkwijze (waarbij je internetverkeer dus níét door hen gelogd wordt), maar absolute zekerheid hierover heb je nooit.

TIP: RICHT JE WERKCOMPUTER IN MET STRIKTE SCHEIDING

Zorg ervoor dat je je werkcomputer strikt indeelt in een privé- en publiek luik. Al te vaak vermengen beide zich (privémails in de werkbox, bestanden in mappen die er niet thuishoren, enzovoort). Je werkgever heeft immers het recht om zich toegang te verschaffen tot je computer (bijvoorbeeld om software te veranderen of bij te werken, of beveiligingsmaatregelen te nemen). Alles wat privé is, zet je in een aparte map met 'PRIVAAT' of 'PERSOONLIJK' als label. Dat maakt zowel voor jou als voor je werkgever duidelijk welke informatie voor wie bestemd is.

Breng je je eigen pc mee, maak dan duidelijke afspraken met de werkgever. Immers: in je privéapparaten mag die niet zomaar binnen. Communicatie is hier — zoals zo vaak — de sleutel.

Ik vermoed dat je op je werk geen camera hangen hebt in de toiletten. Als dat wel zo is, is het hoog tijd om van job te veranderen — en het me even te laten weten. Camera's maken echter wel meer en meer deel uit van het bedrijfsleven. Terwijl ze vroeger gereserveerd waren voor stevig uit de kluiten gewassen bedrijven, dringen ze nu ook — door hun lage kostprijs en geringe complexiteit — binnen bij kleine kmo's. Vaak gaat het dan opnieuw over goedkope IP-camera's, met alle risico's van dien (zie ook 'Privacy bij je thuis').

Mag een werkgever eigenlijk zomaar een camera ophangen? Wel, als het gaat om publiek toegankelijke ruimtes zoals de inkomhal, het parkeerterrein of de stockageruimte, dan zal er op zich weinig aan de hand zijn. Er moet altijd kennis gegeven worden van de camera's (middels de veelgebruikte bordjes), en de camera's moeten aangemeld worden. Die aanmelding gebeurde vroeger bij de Privacycommissie (nu GBA), nu gebeurt dat bij de politie. Jaja, je leest het goed. Het doel daarvan is dat de

politie niet alleen beschikt over een eigen surveillancenetwerk, maar daar ook alle private camera's kan aan toevoegen. Handig bekeken.

Een camera in het toilet, in de lunchruimte, boven je bureau... je voelt het zelf wel aan: dit kan meestal gewoonweg níét. Werk je in de supermarkt en is er sprake van diefstal uit de kassa op geregelde basis, dan kan bijvoorbeeld wel tijdelijk een camera net boven de kassa geplaatst worden. Stiekem kan dit nooit: de werkgever moet hier altijd de bewuste werknemer(s) van op de hoogte brengen.

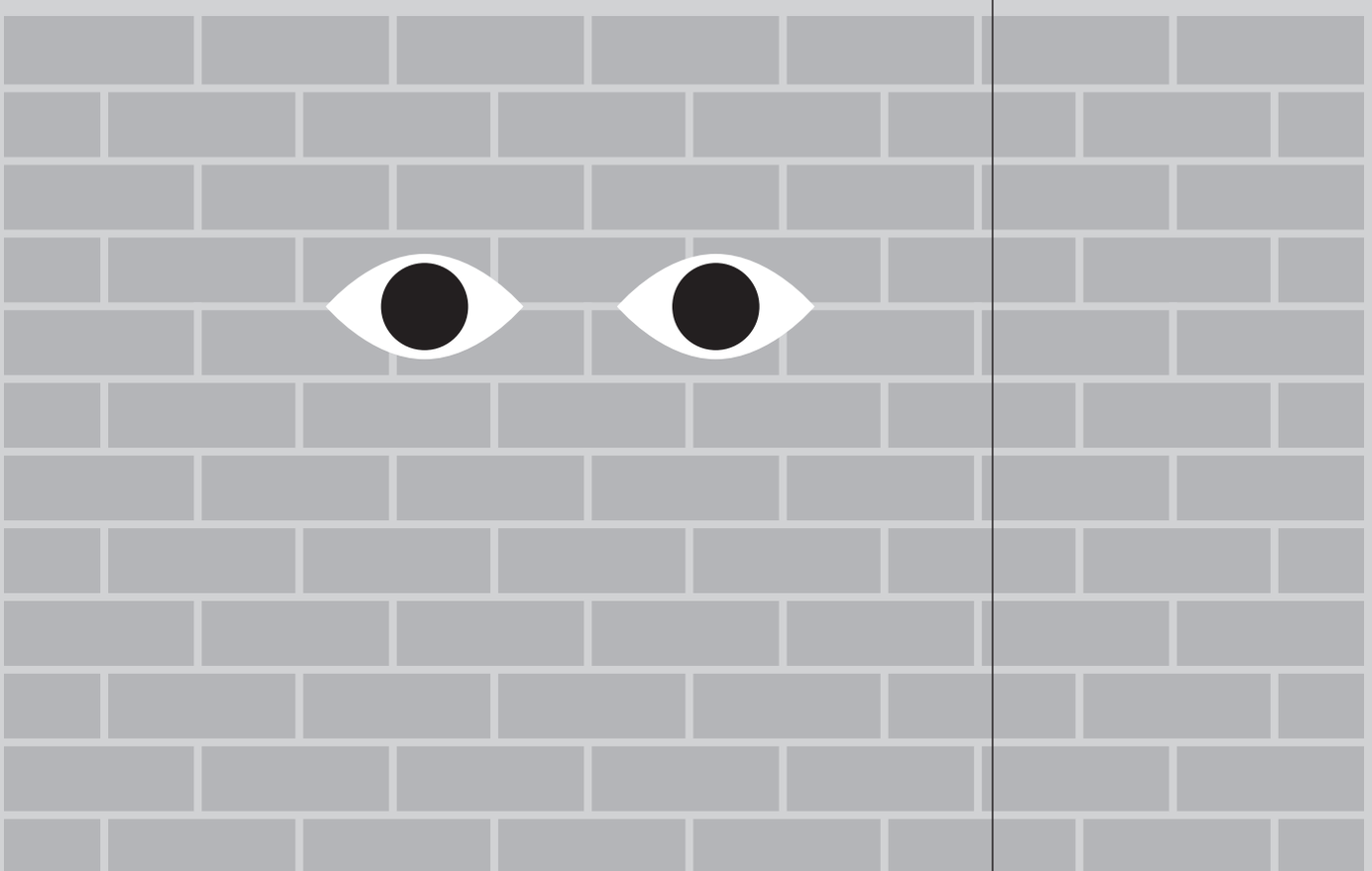
WEETJE: VERHUURDER VEROORDEELD VOOR CAMERA BIJ STUDENTEN

Een verhuurder van studentenkamers had er niets beters op gevonden dan een bewakingscamera te installeren in de gemeenschappelijke keuken. Een van de studenten was hiermee absoluut niet akkoord — ze bestaan nog, de kritische studenten! — en diende klacht in bij de Gegevensbeschermingsautoriteit. De huurder vond de camera een disproportionele inbreuk op haar privacy. De huisbaas verweerde zich door te stellen dat de camera er stond om vandalisme in de studentenkeuken te voorkomen. De GBA maakte korte metten met de zaak: de camera was verboden, de verhuurder moest deze verwijderen, inclusief alle gemaakte beelden. Een van de argumenten van de GBA was dat de huurder geen vrije keuze had: om te eten moest ze de keuken uiteraard betreden. Een waarschuwing voor alle huisbazen, en een motivatie voor kritische studenten.

Een beter idee dan een camera is een goed gesprek over vertrouwen. Maar overtuig je baas daar maar eens van...

Hoofdstuk 4.

Hoe overtuig je iemand van het belang van privacy



Ik heb niets te verbergen.
Als je niets verkeerd doet, heb je niets te vrezen!
Privacy is allang dood, Facebook weet alles.
Mijn gezondheid/veiligheid heeft absolute voorrang op privacy!
Privacy is voor criminelen.

Dooddoeners, stuk voor stuk. Ze blijven echter wel vlotjes meegaan, en in elke privacydiscussie die je na het lezen van dit boek voert ga je ze horen. Had ik een euro gekregen voor elke keer dat ik ze hoorde de voorbije tien jaar, wel, ik was aan het rentenieren en misschien niet aan het schrijven. Helaas: geen miljoenen euro's hier, maar dus wel reden te meer om tegenargumenten te verzinnen.

De vraag is dus: hoe blokkeren we die onwil en misvattingen wat betreft privacy? Komen ze voort uit onwetendheid, naïviteit, intellectuele oneerlijkheid of simpelweg luiheid? Het is moeilijk om daar antwoord op te krijgen, maar wat we wél weten is dat je, als je straks aan de familietafel zit, beter een goed antwoord hebt op deze (drog)argumenten. De beste strategie is níét om er agressief in te vliegen en de beledigingen even rijk te laten stromen als de wijn, maar wel om de situatie om te draaien. Inzicht te brengen in wat — blijkbaar — nog steeds een zeer schimmig en onbekend terrein is. En het is met privacy zoals met alle dingen: onbekend maakt onbemind.

IK HEB NIETS TE VERBERGEN

Ah, de *gouwe ouwe trouwe*. De vaste waarde in het debat. Al moet ik zeggen dat ik het de laatste twee jaar minder en minder frequent tegenkom. Misschien heeft dat wel iets te maken met Edward Snowden. Die antwoordde ooit de legendarisch geworden quote: '*Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.*' De man had er duidelijk wat langer over nagedacht.

bij wetsvoorstellen, bedrijven (die flinke boetes ontvangen sinds de GDPR) en zelfs hopelijk op een dag: bij jou thuis. Misschien draait je kind zich straks wel om als je een foto maakt: 'Hey mama, en mijn privacy dan?' We kunnen maar dromen!

MIJN GEZONDHEID/VEILIGHEID HEEFT ABSOLUTE VOORRANG OP PRIVACY!

Het valse dilemma. Ben je voor privacy, dan ben je tégen de gezondheid van mensen! Een verwijt dat ik al eens kreeg na de terroristische aanslagen: je bent voor privacy, dus voor terroristen! Ja hoor.

Een eenvoudige drogreden, eigenlijk. Het is niet *of-of*, maar *en-en*. We kunnen én zorg dragen voor ieders gezondheid, én daarbij de privacy van elk individu maximaliseren. Dat de twee radicaal tegen elkaar werden uitgespeeld tijdens de coronacrisis, heeft meer te maken met hoe de media werken dan met de realiteit.

Onze media leven van tegenstellingen, teren erop. Niemand wil nog genuanceerde analyses lezen, we willen harde debatten, sterke opinies. Het beste bewijs daarvan is het kiesresultaat. Centrumpartijen verliezen elke keer weer stukjes, terwijl extreme partijen — zowel aan linker- als rechterzijde — gevoelig terrein winnen. Stef Bos zong het al:

> Ik sta hier in het midden
> De wereld om mij heen
> De linkerkant is bloedeloos
> En de rechterkant is leeg
> Wat voor de ene liefde is
> Is voor de ander haat
> Alsof wij zijn vergeten
> Dat het midden nog bestaat

En zo vergaat het ook het privacydebat. Diegenen die oproepen tot nuance worden niet gehoord. Extreme visies worden uitgesmeerd. De waarheid is nochtans eenvoudig: men kan potentiële terroristen traceren door zeer gericht politiewerk, zonder daarbij de hele bevolking te volgen. Het beste bewijs daarvan zijn de talrijke NSA-programma's in de Verenigde Staten, die een verregaande surveillance opzetten en elke Amerikaanse burger konden afluisteren. Hoeveel resultaten boekten dergelijke programma's denk je, de voorbije jaren? Nul. Ik herhaal: nul. Elke terrorist — of minstens geradicaliseerde oproerkraaier — werd in de kraag gevat door ouderwets gericht speurwerk.

Het draait erom een evenwicht te vinden. Een evenwicht waarbij we nooit 100% veiligheid, of 100% gezondheid, kunnen en mogen garanderen. In China is het héél misschien *iets* veiliger (al domineren nieuwsberichten over concentratiekampen vol Oeigoeren, leerkrachten die op systematische wijze hun leerlingen mishandelen en andere misdadige feiten de laatste jaren onze nieuwsagenda), maar je hebt er wel geen enkele vrijheid of verwachting van privacy meer over. Je krijgt automatisch een boete — met behulp van je smartphone, slimme camera's en gezichtsherkenning — als je het rode licht negeert en oversteekt, maar maakt dat een maatschappij zoveel veiliger? Is het het waard om je burgers te behandelen als vee, met een *social credit score*, om absolute veiligheid te bereiken?

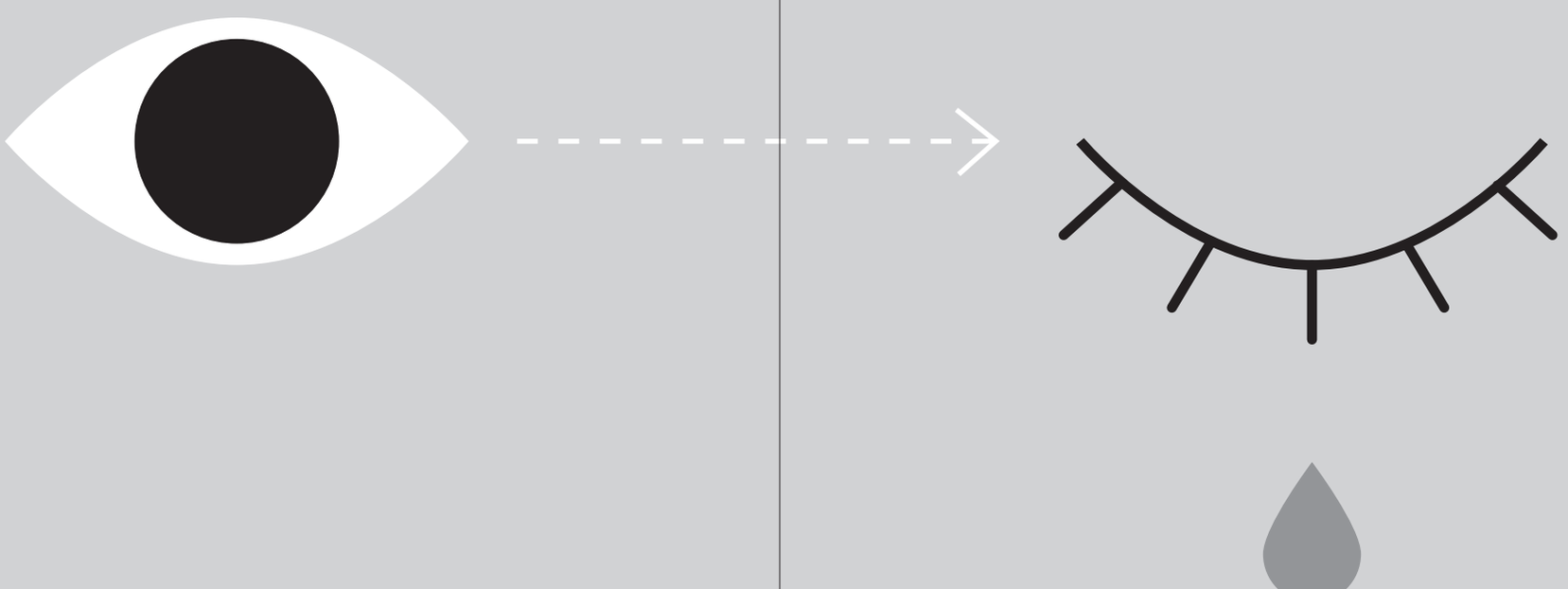
Over gezondheid dan. De corona-applicatie is perfect privacyvriendelijk. Ze is open source, heeft een expliciet wettelijk kader en is niet verplicht maar wel vrijwillig. Mocht elk overheidsproject uitgevoerd worden als die applicatie, ik moest me een ernstige job zoeken. Een combinatie van privacy én gezondheid kan perfect bereikt worden, maar men moet het ook willen.

Geloof niemand die argumenteert met valse dilemma's. Het is weinig meer dan intellectuele luiheid en gemakzucht.

Hoofdstuk 5.

Wat bij een privacyschending?

En hoe neem je een stukje terug?



JE JURIDISCHE TOOLBOX

De komst van de GDPR ging vooral gepaard met de nodige alarmbellen (en pure paniek) bij onze bedrijven. Voor consumenten bleef het bij een hoop (trouwens vaak onnodige) vervelende e-mails van bedrijven waar je al jaren niks meer van hoorde, maar die in je mailbox nu opeens je privacy zalig verklaarden. 'We geven om je privacy', 'we vinden je privacy belangrijk', 'we hebben je toestemming nodig'. Enfin, de marketingjongens en -meisjes waren maar weer eens naar een of andere obscure opleiding geweest, en de mailservers bezweken bijna onder de druk.

Jammer. Heel erg jammer. Weet je waarom? De GDPR (*General Data Protection Regulation* in het Engels, AVG of Algemene Verordening Gegevensbescherming in het Nederlands) bracht net heel wat praktische rechten met zich mee. Wapens, als het ware, die je in stelling kan brengen tegen bedrijven en overheden die je privacy niet naar waarde schatten.

Bij het grote publiek is de GDPR nooit doorgebroken, of toch minstens niet om de juiste redenen. Die cookie pop-ups — die werkelijk iedereen haat, en die bol staan van de leugens (néén, geen enkele krant geeft een halve moer om je privacy, want gemiddeld laten ze zo'n vijfhonderd trackers op je los) — zijn ondertussen vereenzelvigd met de strenge privacywet. Volledig ten onrechte, want cookies worden gevat door andere regelgeving.

Om die kapitale fout én vergissing recht te zetten, durven we het aan om in dit boek een stuk droge wetgeving om te toveren tot echte wapens. *Let's go!*

Recht om vergeten te worden

Een absolute nieuwigheid. *The right to be forgotten* is exact dat wat ze laat geloven: je kan aan bedrijven en overheden simpelweg vragen om alle data die ze je over jou hebben te verwijderen. Boem, weg!

De meer achterdochtige lezer vraagt nu: 'En hoe zijn we daar zeker van?' Ah, dat ben je niet. In grote mate moet je dus vertrouwen op de

Recht op bezwaar

Vind je het niet zo fijn dat bepaalde organisaties je data gebruiken? Dan heb je (quasi) altijd een recht van bezwaar. Simpel voorbeeld: je krijgt een mailing van een of ander commercieel bedrijf en je inbox puilt nu al uit. Onderaan de e-mail zal je vaak een optie vinden om jezelf uit te schrijven ('*unsubscribe*') van de mailinglijst — even los van de vraag of je er op een rechtmatige manier in bent beland. Dat is een eenvoudige geautomatiseerde toepassing van je recht op bezwaar, maar je kan dit dus ook manueel aanvragen bij elk bedrijf dat je data gebruikt voor direct marketing of zelfs voor andere doeleinden. Zo'n verzoek hoeft niets speciaals te zijn. De Autoriteit Persoonsgegevens (Nederland) heeft een verzameling voorbeeldbrieven op haar website staan. Bij het recht op bezwaar, bijvoorbeeld:

> *Onderwerp: direct stoppen met gebruik van mijn persoonsgegevens*
>
> *Geachte heer, mevrouw,*
>
> *U maakt gebruik van mijn persoonsgegevens. Ik maak hiertegen bezwaar en ik verzoek u het gebruik van mijn gegevens door uw organisatie direct te stoppen. De reden van mijn verzoek is ..... [+ uitleg/toelichting].*
> *Ik beroep me voor mijn verzoek op artikel 12 en 21, tweede lid van de Algemene Verordening Gegevensbescherming.*
>
> *Wat vraag ik aan u?*
> *Ik vraag u direct te stoppen met het gebruik van mijn gegevens. Graag ontvang ik van u binnen een maand hiervan een schriftelijke bevestiging.*

Het kan aan de Nederlandse nuchterheid liggen, maar zoals je ziet: veel woorden hoef je er niet aan vuil te maken. *Just do it!*

Ook onze Belgische Gegevensbeschermingsautoriteit heeft trouwens dergelijke standaardbrieven op haar website, al dien je wel iets beter te zoeken (bij 'Burger', 'Wat zijn mijn rechten').

Geautomatiseerde individuele besluitvorming

Afsluiten doen we — zoals het ook betaamt — met een speciaal geval. Je hebt volgens de GDPR het recht om niet te worden onderworpen aan 'volledig geautomatiseerde besluitvorming'. Besluitvorming dus zonder enige menselijke tussenkomst (denk maar aan slimme algoritmes die banken, verzekeraars en operatoren gebruiken om je gedrag in kaart te brengen, risico's te berekenen, enzoverder).

Het blijft een vrij leeg recht, en dat komt eenvoudigweg door al het gelobby rond de totstandkoming van de GDPR. Het is namelijk in drie gevallen toegestaan:

1. Wanneer het noodzakelijk is voor de uitvoering van een overeenkomst tussen het datasubject (jij dus) en de verwerkingsverantwoordelijke.
2. Wanneer het toegestaan is door wetgeving.
3. Wanneer je je toestemming hebt gegeven.

Bijna in alle gevallen zal zo'n geautomatiseerde individuele besluitvorming dus toegelaten zijn. Denk maar aan contracten of algemene voorwaarden die je ondertekende bij je bank of verzekeraar, je toestemming (dat knopje 'Ik ga akkoord' waarvoor iedereen ondertussen zodanig is geconditioneerd om er onmiddellijk op te klikken), enzoverder.

Lobby in wetteksten is een groot probleem, en eentje waar in het bijzonder het Europese niveau last van heeft — waar lobbyisten een fulltime job hebben, die ook nog eens goed betaald is, om Europese parlementsleden te verleiden tot het aanpassen of zelfs volledig heropstellen van wetgeving. De GDPR was (en is) geen uitzondering. Helaas.

JE TECHNISCHE TOOLBOX

Je rechten kennen is mooi, maar ze kunnen uitoefenen is mooier. Hoewel de grote techbedrijven er niet mee te koop lopen — het gaat immers in tegen hun businessmodel — hebben vele van hen sinds de komst van de GDPR privacytools geïntroduceerd. Neem dat wel met een korreltje zout: meer dan aan de minimumvereisten zullen ze niet snel voldoen. Het kan echter geen kwaad om naast je juridische toolbox ook je technische toolbox uit te breiden. Op één paard wedden is nooit verstandig.

Hieronder behandelen we de grootste techbedrijven en -netwerken. Belgische bedrijven hebben soms ook portalen (bijvoorbeeld Immoweb of 2dehands.be), maar ze allemaal behandelen leidt ons te ver. Kijk goed in je gebruikersaccount voor 'privacyinstellingen' en pas aan waar nodig of gewenst.

Google

Als er één bedrijf is dat veel te veel weet over ieder van ons — en dus inderdaad *weet wie je bent en wat je doet* —, dan is het Google. Ooit opgericht met de slogan '*don't be evil*' (in 1999 door Google-ontwikkelaar Amit Patel). In 2018 sneuvelde het motto, verbannen naar een obscure zin op het einde van de *code of conduct*.

Google is een doorn in het oog van veel privacyactivisten en de reden daarvoor is eenvoudig: het bedrijf heeft geen ander businessmodel dan het verwerken, opslaan en verkopen van onze privé-informatie. In tegenstelling tot bijvoorbeeld Apple, dat zich — zolang het tenminste dure apparatuur van duizenden euro's kan blijven slijten — opwerpt als techhoeder van onze privacy. In hoeverre die claims van Apple correct zijn is soms maar moeilijk na te gaan, maar het valt inderdaad op dat het bedrijf de laatste jaren verschillende ingrijpende wijzigingen heeft aangebracht in het besturingssysteem van iPhone (iOS) die de privacy van gebruikers beter moeten beschermen.

Google dus. Zijn zoekmachine is het best gekend en *oh boy*, daar geven we ons hele leven in. Hoe we ons voelen, onze onzekerheden, of we ziek

of gezond zijn, onze nieuwe hobby, hoeveel keer we zoeken naar onze ex, onze ambities, onze jobdromen, *wie we zijn*.

Die zoekmachine is lang niet het enige product in het arsenaal van moederbedrijf Alphabet. De populaire e-mailsoftware Gmail scant e-mails op advertentiewoorden, Google Maps (en ook Waze) scant onze verplaatsingen en houdt die netjes bij, YouTube weet waar we naar kijken en Chrome, de webbrowser die het overgrote marktaandeel heeft, tja, die weet perfect naar welke websites we surfen.

Tijd dus om hier iets aan te doen.

Google introduceerde een Privacycheck (myaccount.google.com/data-and-personalization), waar je je activiteitsopties kan beheren. Standaard staat alles op 'Aan', waardoor je web- en appactiviteit, locatiegeschiedenis, YouTube-geschiedenis en browserhistoriek allemaal netjes naar de servers van Google gaan. Eerste stap: alles uitschakelen. Als je YouTube-aanbevelingen handig vindt, kan je die bijvoorbeeld aanlaten. Zet zoveel mogelijk uit is wel de tip.

Klik je op 'Locatiegeschiedenis uitzetten', dan is het niet zo dat Google géén data meer opslaat — stel je voor! Je krijgt de keuze tussen 'activiteit ouder dan 3 maanden automatisch verwijderen', 'ouder dan 18 maanden' en 'ouder dan 36 maanden'. Grijns. Te makkelijk mag het niet worden, toch? Het bedrijf verdedigt die keuze op basis van het 'gerechtvaardigd belang' dat het heeft om jou beter te kunnen bedienen gedurende die drie maanden.

Echter vooraleer je aan instellingen begint te morrelen, is het interessant om eens te bekijken wat Google tot nu toe over jou heeft vergaard. Via het Google Dashboard ('Wat je maakt en doet' — een louter toevallige gelijkenis met de titel van dit boek) krijg je een massaal overzicht van je data. Klik daar op 'Download je gegevens' ('Google Takeout').

Mijn Google Takeout was een kopie van bestanden in maar liefst 52 (!) producten. Het duurde ongeveer een halve dag voor het mailtje van Google binnenkwam. In de Takeout was maar liefst 9,21 gigabyte aan