THEY'RE WATCHING

E-magazine
Jaargang 6
Editie 1, 2019/2020

Law & ICT Students' Association LISA

Brinkhof

Dirkzwager legal & tax

NORD ADVOCATEN

Hoofdredacteur
Bas Smits

Redacteur/Vormgever
Joyce Bruinewoud

Redacteur
Iris Haringsma

Redacteur
Caitlin Verhoeven

VOORWOORD

BESTUUR

Beste leden, lezers en geïnteresseerden,

Het eerste E-magazine van het jaar ligt alweer voor u, een mijlpaal in het jaar. Na het zeer geslaagde symposium in november gaat ook dit E-magazine in op een van de belangrijkste onderwerpen van onze opleiding: privacy. Voor mijn gevoel is dit onderwerp bij de grote massa pas doorgedrongen toen de media over de AVG begonnen te berichten, wat pas echt ging lopen in de loop van 2017. Een echte angstgegner vormt deze verordening, in de volksmond ook wel 'die AVG-wet' genoemd of, zoals ik zelfs eens hoorde, de 'AGV'.[1] Door deze AVG-angst durft niemand meer persoonsgegevens te delen, op te schrijven of te bewaren.

Aan de andere kant wordt alleen de verwerkingsgrond van toestemming te pas en te onpas gebruikt, ook waar dat niet altijd even relevant is. Dat onder andere een gerechtvaardigd belang als grond voor verwerking kan gelden, heeft men blijkbaar niet door. Gelukkig is de redactiecommissie er weer goed in geslaagd om dit voor veel mensen lastige onderwerp helder en begrijpelijk in een mooi E-magazine te verwerken, waarvoor chapeau!

Namens het zeventiende bestuur,

Auke-Frank Tadema
Voorzitter

1 De Fryske Vlogger, 'Bedreigd op de markt in Leeuwarden', https://youtu.be/yXzMYvVCLZc.

VOORWOORD

HOOFDREDACTEUR

Beste lezer,

Voor u ligt alweer het eerste E-magazine van het jaar. De nieuwe redactiecommissie is de afgelopen maanden druk geweest om de meest interessante rechtsontwikkelingen aan te kaarten; niet alleen in Nederland, maar verspreid over de wereld. Achter de schermen heeft de gehele commissie hard gewerkt aan dit magazine. Ik wil dan ook even dit moment aangrijpen om de rest te bedanken voor hun geweldige inzet van de afgelopen tijd!

Zoals de titel al doet vermoeden, gaat 'They're watching' over een van de belangrijkste onderwerpen in het IT-recht: privacy. In aansluiting op het symposium hebben wij geprobeerd om wat duidelijkheid te scheppen in de afweging tussen privacy en opsporing. Dit onderwerp zorgt zelfs binnen onze eigen commissie al voor de nodige meningsverschillen, wat al aangeeft hoe erg de meningen hierover uiteen kunnen lopen.

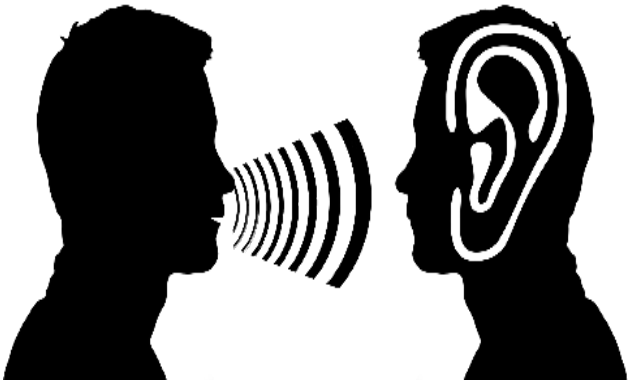
Ik hoop dat het voor uzelf, na het lezen van 'They're watching', toch wat duidelijker is geworden waar de nadruk hoort te liggen. Op zijn minst hoop ik dat u het magazine met veel plezier zal lezen.

Namens de redactiecommissie,

Bas Smits
Hoofdredacteur

INHOUDSOPGAVE

Oren in je slaapkamer



'Afluisteren? Maakt mij niet uit, ik heb niks te verbergen.' Dat zal het antwoord zijn van menigeen die gevraagd wordt of afluistering met het oog op veiligheid of functionaliteit diegene hindert. Maar maakt het je wel uit als de persoon die ernaar luistert alles kan horen wat zich in je woonkamer en slaapkamer afspeelt? Afgelopen juli werd duidelijk dat medewerkers van Apple via Siri medische gegevens, seksgeluiden en criminele activiteiten te horen kregen om zo de dienst te verbeteren.[1] Niet alleen Siri maakt zich hieraan schuldig, ook Amazons Echo en Googles Alexa luisteren je af.[2] Mag dit allemaal wel?

Niks nieuws

Het afluisteren door middel van alledaagse technologie is geen nieuw fenomeen. Zo kan je je misschien nog de app Talking Angela herinneren, die in opspraak kwam, omdat in de ogen van de pratende kat een man zou zitten die je via je camera zou opnemen. Duizenden boze reviews, YouTube-filmpjes en bezorgde ouders verder bleek dit allemaal een hoax te zijn.[3] Na Talking Angela kwam in 2017 naar voren dat er zo'n 250 (!) apps in de Google Playstore staan, die je microfoon ook buiten gebruik van de app kunnen aanzetten om bijvoorbeeld te tracken naar wat voor televisieprogramma's je kijkt, zodat daarop advertenties kunnen worden aangepast.[4] Dit betreffen vaak apps waarvoor je je microfoon nodig hebt, dus waar je ook instemt met het gebruik van de microfoon. Via jouw 'toestemming' (die toestemming waarbij je maar snel op 'ok' drukt om je nieuwe spelletje te kunnen spelen) kunnen ze dan ook luisteren naar omgevingsgeluiden en data over je verzamelen. Naast het afluisteren hebben ze nog iets gemeen: ze maken allemaal gebruik van de software van Alphonso, een bedrijf dat TV-kijkgegevens verzamelt en die vervolgens doorverkoopt aan adverteerders. Het zijn trouwens niet de onbekende apps die je data verzamelen. Zo komen Goodreads, Wikihow en TED voor op de lijst van apps die Alphonso gebruiken.[5] Misschien denk je nu: ha, maar ik heb Apple, dus mij overkomt dat niet. Dat is echter niet helemaal waar. Het is niet geheel duidelijk welke apps

1 NU.nl (2019). Apple beluistert Nederlandse Siri-opnames, bedrijf stopt met project. Geraadpleegd van https://www.nu.nl/tech/5973329/apple-beluistert-nederlandse-siri-opnames-bedrijf-stopt-met-project.html.

2 Ng, A. (2019, 21 oktober). Alexa and Google Assistant fall victim to eavesdropping apps. Geraadpleegd op 1 december 2019, van https://www.cnet.com/news/alexa-and-google-voice-assistants-app-exploits-left-it-vulnerable-to-eavesdropping.

3 Dredge, S. (2014, 20 februari). What the Talking Angela app is really saying to your kids. Geraadpleegd op 1 december 2019, van https://www.theguardian.com/technology/2014/feb/18/talking-angela-app-children-safety.

4 Maheshwari, S. (2017, 28 december). That Game on Your Phone May Be Tracking What You're Watching on TV. Geraadpleegd op 1 december 2019, van https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.

5 Lijst gevonden op https://play.google.com/store/search?q=%22alphonso%20automated%22&hl=en.

uit de App Store werken met Alphonso, omdat dit minder goed vindbaar is. Wel is duidelijk dat Apples Shazam een overeenkomst heeft met Alphonso, waarbij Shazam jouw opgezochte muziek uit bijvoorbeeld films of reclames doorverkoopt aan Alphonso. Je Apple-apparaat is dus ook niet volkomen veilig.[6]

Sneaky

Kan dit allemaal zomaar? Alphonso CEO Ashish Chordia rechtvaardigt het afluisteren door te stellen dat de consument zelf instemt met het gebruik van de microfoon en bovendien het gebruik van de microfoon ook altijd weer kan uitzetten.[7] In principe heeft de CEO gelijk. Wanneer je je microfoon moet gebruiken voor een spelletje, word je standaard gevraagd of je de app toegang tot je microfoon wil geven. Toch geef je hiermee niet ook gelijk toestemming voor het gebruik van de microfoon buiten het gebruik van de app. Apps die je gegevens via je microfoon verzamelen, dekken zich dan ook vaak in via hun gebruikersvoorwaarden. Neem bijvoorbeeld de app Beer Pong: Trickshot. In de algemene voorwaarden stelt de maker het volgende: 'We may use some third parties, which helps us to collect, store and process the information'.[8] Ze kúnnen de data dus samen met derden verzamelen.

Risico's

Oké, prima. Ze luisteren ons dus af en weten naar welke televisieprogramma's we kijken, maar wat dan

nog? De mogelijkheden van het afluisterende programma zijn niet alleen voor de app-ontwikkelaars functioneel; hackers weten er ook wel raad mee. Zo kunnen hackers in de hoedanigheid van app-ontwikkelaar apps maken voor de slimme speaker en met die apps ervoor zorgen dat je speaker je afluistert. Dit bewerkstelligen ze door na een commando van de gebruiker een lange stilte te laten vallen, waardoor je denkt dat de app is afgesloten. De app blijft echter langer luisteren en zolang jij elke 30 seconde iets zegt, blijft de app open. Doordat jij iets zegt, blijft de app namelijk luisteren of het commando's krijgt. Wat jij vervolgens zegt, wordt teruggestuurd naar de ontwikkelaar en zo kan de ontwikkelaar hele gesprekken van je binnenkrijgen.[9]

Bovendien kunnen hackers door middel van speakerapps de functionaliteiten van de homespeakers uitbreiden. Gebruikers van de speaker kunnen de app openen door bijvoorbeeld te zeggen 'Google, open My Horiscope' en de gebruiker kan dan vervolgens een actie noemen binnen de app,

6 Van der Zwaag, G. (2018, 4 december). Apple's Shazam werkt mee aan games die je tv-kijkgedrag afluisteren. Geraadpleegd op 1 december 2019, van https://www.iculture.nl/nieuws/alphonso-shazam.

7 Van der Zwaag, G. (2018, 4 december). Apple's Shazam werkt mee aan games die je tv-kijkgedrag afluisteren. Geraadpleegd op 1 december 2019, van https://www.iculture.nl/nieuws/alphonso-shazam.

8 Dumado Games. (2018, 18 september). Privacy Policy. Geraadpleegd op 3 december 2019, van https://dumadu.com/privacy-policy.

9 Carlos, N. (2019, 21 oktober). Alexa, Google Home Used As 'Smart Spies' By Malicious Apps To Eavesdrop And Phish For Passwords. Geraadpleegd op 1 december 2019, van https://www.techtimes.com/articles/245771/20191021/alexa-google-home-used-as-smart-spies-by-malicious-apps-to-eavesdrop-and-phish-for-passwords.htm.

die daarop wordt uitgevoerd. Een hacker kan hierbij als respons kiezen dat de speaker erg lang stil blijft en vervolgens zegt dat er iets misgaat, waarbij het vervolgens om je wachtwoord vraagt. Wat je hierop reageert, wordt rechtstreeks teruggestuurd naar de app-ontwikkelaar en daarmee is je wachtwoord ook bij hem. Ja, Google en Amazon testen of de app wel veilig is. Men kan echter na deze test de app aanpassen en weer onveilig maken. De app wordt namelijk niet twee keer getest.[10]

AVG

Met de recente intreding van de Algemene Verordening Gegevensbescherming zou men denken dat het afluisteren niet is toegestaan. Het lijkt namelijk nogal in strijd te zijn met het recht op privacy. Het zit hem, zoals eerder al genoemd, echter in het geven van de toestemming. Op grond van artikel 6 lid 1 AVG maakt het geven van toestemming door de betrokkene dat de gegevensverwerking rechtmatig is. Eventueel zou de afluistering stuk lopen op artikel 5 AVG, dat voorschrijft dat de verwerking rechtmatig, behoorlijk en transparant moet zijn. Bovendien moeten volgens datzelfde artikel de persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen ze vervolgens niet op een met die doeleinden onverenigbare wijze worden verwerkt. Vooral de transparantie lijkt bij apps soms ver te zoeken, met name bij de algemene voorwaarden van de app. Zodra je de app downloadt, ga je met het gebruik van je microfoon en de datacollectie door de app akkoord en pas als je de algemene voorwaarden van de app bekijkt, zie je wat ze allemaal van je verzamelen en voor welk doel ze dit doen. Met deze voorwaarden wordt dus voldaan aan de AVG.[11] Dus elke keer dat je een app downloadt en je deze toestemming geeft voor bijvoorbeeld toegang tot contacten, foto's of je microfoon, ben je het slachtoffer van het verzamelen van data. Dit is echter wel in overeenstemming met de AVG, omdat de algemene voorwaarden de gegevensverwerking behandelen, ook al leest niemand ze.[12]

Californische wet

Toch komt Apple er niet zomaar mee weg. In augustus 2019 is Apple aangeklaagd voor het handelen in strijd met California's Invasion of Privacy Act, de Unfair Competition Law, de Consumers Legal Remedies Act en de Declaratory Judgment Act. De aanklager beschuldigt Apple in vier eisen ervan dat het onrechtmatig en bewust vertrouwelijke gesprekken van personen opneemt zonder hun toestemming.[13] Volgens art. 632 van de privacywet van Californië is het afluisteren van een vertrouwelijk gesprek inderdaad illegaal.[14] Bovendien stelt de aanklager dat de algemene voorwaarden van Apple niet verwijzen naar het opslaan van de opnames en dat deze gesprekken worden beluisterd door de medewerkers.[15] Daarmee handelt het ook in strijd met de Consumers Legal Remedies Act.[16] Oftewel, het wordt een lastige zaak voor

10 SRLabs. (2019, 20 oktober). Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping – Security Research Labs. Geraadpleegd op 1 december 2019, van https://srlabs.de/bites/smart-spies.

11 Verordening (EU) 2016/679.

12 Joseph, C. (2019, 7 maart). Is this proof your smart phone is eavesdropping on EVERY single word you say? Geraadpleegd op 1 december 2019, van https://www.dailymail.co.uk/news/article-6765113/Is-proof-smartphone-eavesdropping-single-word-say.html.

13 Miller, C. (2019, 7 september). Apple hit with Siri lawsuit. Geraadpleegd op 1 december 2019, van https://9to5mac.com/2019/08/07/siri-lawsuit-recordings.

14 California Code, Penal Code - PEN § 632 | FindLaw. (z.d.). Geraadpleegd op 1 december 2019, van https://codes.findlaw.com/ca/penal-code/pen-sect-632.html.

15 Fumiko Lopez v. Apple inc, 5:19-cv-04577 (Northern district of California 2019). Te vinden op https://www.courtlistener.com/recap/gov.uscourts.cand.345934/gov.uscourts.cand.345934.1.0.pdf#cjwg.

16 Consumers Legal Remedies Act (1970). Te vinden op https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.5.&part=4.&chapter=3.&article=.

Apple. Apple heeft als gevolg hiervan het opnemen van de gesprekken geschorst en is een intern onderzoek gestart naar het opslaan en luisteren van de opnames. Er kan dus zeker wat aan gedaan worden. Het is nog niet duidelijk wanneer de zaak zal plaatsvinden, maar de uitkomst zal vast interessant zijn, aangezien het ook effect kan hebben op andere bedrijven met spraakassistenten.

Technologie dan maar weggooien?

Mocht je een app willen downloaden, die ondersteund wordt door Alphonso, denk dan nog eens twee keer na. Er is een grote kans dat de app vaker meeluistert dan alleen op het moment dat jij tegen de app praat. Bovendien lijken slimme speakers zich daar ook aan vuil te maken, waar derde-ontwikkelaars weer profijt van kunnen hebben. De AVG biedt je als consument dan geen bescherming, want via de algemene voorwaarden en jouw toestemming voldoen de apps toch aan de gestelde privacyeisen. Een lichtpuntje is dat Amerikaanse wetten de afluisterpraktijken wél verbieden en er zo misschien voor gaan zorgen dat de medewerkers van de bedrijven, hopelijk ook bij ons, niet meer met je persoonlijke gesprekken kunnen meeluisteren. We wachten de rechtszaak tegen Apple in spanning af.

Namens de redactiecommissie,

Iris Haringsma

Interview met mr. Vivienne Verlinden-Masson

Zou u zich willen voorstellen?

Mijn naam is Vivienne Verlinden-Masson. Ik ben advocate, gespecialiseerd in het IT-recht, IE-recht en privacyrecht. Ik ben in 1989 begonnen met de advocatuur in Amsterdam. 1,5 jaar later ben ik naar het noorden verhuisd en ben ik bij PlasBossinade in Groningen aan de slag gegaan.

Waarom heeft u gekozen voor deze specialisatie?

Dit was eigenlijk puur toeval. Mijn patroon (een ervaren advocaat die een advocaat-stagiaire moet opleiden) in Amsterdam was actief in het intellectueel eigendomsrecht en daardoor rolde ik er ook automatisch in. Na mijn verhuizing hield ik me in Groningen daar ook weer mee bezig. Het IT-recht was toen nog heel erg in ontwikkeling. Als er daarom een vraag rees met betrekking tot IT werd er bij mij aangeklopt.

Wat heeft u na uw studie gedaan?

Nadat ik was afgestudeerd had ik het gevoel dat ik nog niet zoveel van de praktijk wist. Daarom ben ik een postdoctorale opleiding gaan volgen aan de Grotius Academie. Dit was toen een eenjarig full-time programma met 8 verschillende modules. Dit was hard werken. Ik kreeg praktijk vraagstukken voorgeschoteld over onderwerpen waar ik nog niet zo bekend mee was. Over de periode van één dag moest ik mij vervolgens oriënteren op dit onderwerp, het van zoveel mogelijk kanten benaderen én er een verslag over schrijven met een goede conclusie. Daarna ben ik het beroepsleven in gegaan.

Is de advocatuur een uitdaging?

Zeker en dat is ook het leuke aan de advocatuur, je moet jezelf blijven ontwikkelen. Bij elk vraagstuk moet je weer kijken of er nieuwe regelgeving of inzichten zijn en bij elke zaak moet je weer opnieuw de stand van zaken bekijken en je positie inschatten.

Hoe ziet uw dag eruit?

Ik zit vrij veel op het kantoor. Dan ben ik bijvoorbeeld bezig met het maken of het beoordelen van contracten en het beoordelen of iemand inbreuk maakt op de IE-rechten van een andere partij.

Verder voer ik besprekingen met cliënten en heb ik zittingen. Ik heb ongeveer twintig tot veertig lopende zaken tegelijk. Ik moet dan ook steeds prioriteiten stellen en goed communiceren met mijn cliënten. Op dagelijkse basis ben ik dan bezig met de zaken die op dat moment de hoogste prioriteit hebben, ofwel omdat je een reactie hebt toegezegd ofwel omdat er een deadline speelt.

Heeft u wel eens zaken waarin u geen idee heeft waar het over gaat?

Jazeker. Er wordt niet van je verwacht dat je bij elke zaak parate kennis hebt van de business van je cliënt. Vaak vraag ik gewoon aan cliënten om hun product of dienst en de specifieke situatie uit te leggen. Dan ga ik vervolgens kijken of er een juridische basis is voor hun zaak en dan komen we er samen wel uit. Bovendien vraag ik wel eens deskundigen om advies en lees ik mezelf bij elke zaak opnieuw grondig in.

Verliest u wel eens zaken en hoe gaat u daarmee om?

Iedereen verliest wel eens een zaak, rechters blijven immers mensen. Het is natuurlijk niet leuk om een zaak te verliezen, maar je weet meestal de uitkomst van een zaak wel in te schatten. Soms weet je al dat de zaak moeilijk te winnen valt en dan moet je dat ook gewoon duidelijk maken aan de cliënt. Je moet cliënten immers beschermen. Bovendien sta je daar niet als partij, maar als vertegenwoordiger waardoor het anders is.

Heeft u er wel eens over nagedacht om iets anders te doen?

Die vraag stel ik mezelf om de vijf jaar weer, maar elke keer kom ik tot de conclusie dat dit het leukste vak is wat er bestaat, dus nee. Ik heb wel eens nagedacht om bij de rechterlijke macht te gaan, maar de advocatuur vind ik toch te leuk.

Waarom bent u advocaat geworden?

Ik ben eerst begonnen als biologiestudent. Na evaluatie van het eerste jaar kwam ik erachter dat dit echter geen studie voor mij was. Toen ben ik rechten gaan studeren en ik heb daarmee een hele goede keuze gemaakt. De advocatuur sprak mij aan omdat het zo divers is.

Werkt u ook met anderen aan een zaak?

Meestal werk je alleen aan een zaak. Bij grotere zaken werken we soms wel met meerdere mensen aan één zaak. Verder hebben we bij PlasBossinade ook advocaat-stagiaires die met ervaren advocaten meelopen en uitzoekwerk doen en concepten schrijven. Bovendien loop ik bij zaken die verschillende rechtsgebieden betreffen vaak bij een collega binnen om zijn of haar kijk op de zaak te vragen. Dus uiteindelijk werk je niet alleen.

Hoe lang duurt een zaak ongeveer?

Dat is heel divers. Sommige zaken zijn in een paar maanden klaar en andere zaken lopen jaren. Mijn langste zaak duurde ongeveer 10 jaar. Dit komt vooral voor bij bodemprocedures en als je in hoger beroep gaat en het hof de zaak dan weer naar een ander hof verwijst. Dan ben je zo alweer een paar jaar verder. Maar ook het wachten op de stukken van de tegenpartij kost tijd, zo heeft een partij drie maanden de tijd om een memorie van grieven op te stellen. Het is voor cliënten vaak een opluchting als de zaak achter de rug is. Zij kunnen er dan ook

eindelijk een punt achter zetten. Omdat een procedure heel belastend kan zijn, kijk je ook altijd of er een schikkingsmogelijkheid bestaat.

Met wat voor cliënten en zaken heeft u vaak te maken?

Voornamelijk bedrijven en instellingen. Ik heb over het algemeen veel zaken op het gebied van het intellectueel eigendom en ICT, zoals het onrechtmatige gebruik van foto's. Bovendien houd ik me veel bezig met licentiecontracten, dus bedrijven die een nieuw contract willen aangaan of juist van hun oude contract af willen.

Wat kunt u toekomstige IT-advocaten aanraden?

Wat ik persoonlijk miste in mijn opleiding was economische kennis. Bij het werken met ondernemingen is dat toch wel handig om te hebben. Dat heb ik dus bij moeten leren. Bovendien is het essentieel om goede kennis omtrent algemeen civiel recht te hebben, óók als je je specialiseert in het IE- of ICT-recht!

Wij willen mevrouw Verlinden hartelijk bedanken voor het interview!

‘Grapperhaus joined the group’

Het is ook nooit genoeg. Vlak na het aannemen van een nieuwe wet, die het mogelijk maakt voor de politie om te hacken, wil Grapperhaus nog meer. Hij wil met grote techbedrijven een afspraak maken dat zij een sleutel kunnen vorderen om chatberichten te kunnen lezen.[1] Deze zijn namelijk momenteel beveiligd met end-to-end-encryption, waardoor de politie er zelf niet bij kan. De grote bedrijven hebben dit tot nu toe niet gedaan, omdat ze de privacy van hun gebruikers willen beschermen.

Wat is end-to-end-encryption?

Om maar bij het begin te beginnen, hoe zit dat end-to-end-encryption (E2EE) nou precies in elkaar? E2EE is een vorm van cryptografie, die berichten die we elektronisch versturen (via WhatsApp, Facebook, Messenger etc.) versleutelt. Het is van belang om te beseffen dat het bericht dat je verstuurt via een server moet gaan, die verzender en ontvanger met elkaar verbindt, voordat het bij de ontvanger aankomt. Het zou onwenselijk zijn als die server alle communicatie tussen beide partijen kan inzien. Wat E2EE doet, is het bericht versleutelen, zodat de server alleen dat versleutelde bericht ziet. De manier om het te ontgrendelen, is met een speciale sleutel. Die sleutel wordt bepaald aan de hand van een wiskundige formule. Ik zal de hele wiskunde erachter achterwege laten, maar enig inzicht in hoe het systeem precies werkt, is wel handig.[2]

Zowel A als B hebben een eigen privésleutel en de server zelf heeft er ook een. Laatstgenoemde is algemeen bekend, maar de overige twee sleutels zijn alleen bekend bij A respectievelijk B: ze weten ook elkaars sleutel niet. Er wordt eerst aan beide kanten een berekening gedaan met A en de publieke sleutel en B met de publieke sleutel. De uitkomsten hiervan zijn zodanig dat de specifieke waarde van A en B niet meer te achterhalen is. Deze uitkomsten worden dan uitgewisseld. Dit komt dus wel op de server terecht en is dus een potentieel doelwit voor hackers en/of Grapperhaus, maar dit is niet erg. Zodra de uitkomst van A op het toestel van B terecht is gekomen (en vice versa), wordt er namelijk nog een laatste berekening uitgevoerd met de sleutel van B op zijn toestel (en uiteraard het omgekeerde voor A). Uiteindelijk zullen zowel A als B tot hetzelfde eindresultaat komen, waardoor A een bericht kan versleutelen met deze sleutel en veilig kan verzenden naar B.

Het voordeel hiervan is dat zowel het versleutelen als het

1 Rudy Bouma, “Minister Grapperhaus wil toegang tot chat en berichtendiensten”, 3 november 2019, te vinden op www.nos.nl (laatst geraadpleegd op 1 december 2019).

2 Voor de geïnteresseerden: dit principe heet het “Diffie-Hellmanprotocol”. Door zelf te Googlen komt men op de uiteindelijke formule uit.

ontsleutelen zich op de computers/telefoons van de eindgebruikers afspeelt. De sleutel en de tekst zelf komen op deze manier nooit op het publieke domein terecht. Wanneer een derde de tekst wil achterhalen, moet ze voor elke gebruiker opnieuw de sleutel "kraken". Dit is in theorie wel mogelijk, maar zelfs met de grootste en beste computers duurt dit te lang om het nog bruikbaar te maken.

Wat wil Grapperhaus?

Dan weer even terug naar de opmerking van Grapperhaus, wat is zijn idee? Hij wil dat de grote techbedrijven een mastersleutel maken, die door justitie gevorderd kan worden bij ernstige verdenken van zware misdrijven, zoals bijvoorbeeld kinderporno.[3] Hij is niet de eerste die dit idee heeft. In de Verenigde Staten heeft de minister van Justitie, William Barr, ook al een pleidooi gehouden dat Facebook een achterdeur moet maken in zijn systeem voor de Amerikaanse overheid.[4] Volgens Barr zorgen de grote techbedrijven, door hun berichten te versleutelen met E2EE, ervoor dat de politie daardoor minder informatie kan vergaren en criminelen sneller de vrije hand wordt gegeven.

Dit laatstgenoemde is zeker waar. Doordat bedrijven aan hun klanten garanderen dat hun communicatie veilig en beschermd is, neemt de criminaliteit toe. In de app Telegram worden bijvoorbeeld verscheide "diensten" in openbare groepen aangeboden. Toen ik zelf de app downloadde, kwam ik binnen een paar minuten al een paar wapenhandelaren, meerdere phishing-sitemakers en te veel drugshandelaren om te tellen tegen. Door deze makkelijke en gebruiksvriendelijke manier wordt het eenvoudiger om online misdrijven te plegen, zo concludeert de Nationale Coördinator Terrorismebestrijding en Veiligheid.[5] Dat Grapperhaus hier tegen wil optreden, is dan ook meer dan logisch!
Hier komt dan echter de keerzijde naar voren. Artikel 8 EVRM, het recht op privacy. Dat elke burger recht heeft op veilige communicatie, die niet zomaar door derden gelezen kan worden, behoeft geen betoog. Dit is al zo sinds het in 1848 grondrechtelijk beschermd werd in artikel 13 van de grondwet. Evenmin behoeft het betoog dat in geval van ernstige inbreuk op de rechtsorde de politie deze privacy opzij kan zetten. Zolang dit aan de noodzakelijkheidstoets van artikel 8 lid 2 EVRM voldoet, moet justitie de mogelijkheid hebben om in te grijpen.

Wat Grapperhaus nu echter wil, veroorzaakt een veel groter probleem. Dat de privacy van een (potentiële) crimineel geschonden wordt, kan in bepaalde gevallen dan wel geoorloofd zijn, maar het moet niet zo zijn dat de privacy van alle burgers geschonden wordt. Dat zal wel gebeuren wanneer Grapperhaus zijn zin krijgt. Als er een "achterdeurtje" of een "master-key" wordt gemaakt, kan de veiligheid van de encryptie niet meer gewaarborgd worden. Juist dat wat E2EE zo veilig maakt, is het feit dat zowel het versleutelen als het ontsleutelen op de privételefoon van de eindgebruikers gebeurt. Het is daarom niet rendabel om bij elke gebruiker apart het bericht te willen ontcijferen; dit duurt simpelweg veel te lang. Bij dat wat Grapperhaus voorstelt, zal dit hele proces maar één keer moeten gebeuren. Daarna hebben ze immers een masterkey waarmee ze álle berichten kunnen ontcijferen die verstuurd worden .

Privacyorganisaties reageren op dit nieuws zoals je zou verwachten. Bits of Freedom stelt dat er niks veranderd is sinds de laatste keer dat deze discussie gevoerd werd.[6] Deze

3 Rudy Bouma, "Minister Grapperhaus wil toegang tot chat en berichtendiensten", 3 november 2019, te vinden op www.nos.nl (laatst geraadpleegd op 1 december 2019).

4 The New York Times, "Bar Pushes Facebook for Access to WhatsApp messages", 3 oktober 2019, te vinden op www.nytimes.com (laatst geraadpleegd op 1 december 2019).

5 Nationaal Coördinator Terrorismebestrijding en Veiligheid, "Cybersecuritybeeld Nederland CSBN 2019", 12 juni 2019, p. 27, te vinden op https://www.rijksoverheid.nl (laatst geraadpleegd 1 december 2019).

6 Rejo Zenger, "Grapperhaus irriteert met gebrek aan kennis over eigen beleid", 4 november 2019, te vinden op www.bitsoffreedom.nl (laatst geraadpleegd 1 december 2019).

discussie kwam namelijk eerder al naar voren, maar het kabinet heeft in 2016 in zijn beleid vastgelegd dat het niet wenselijk is om beperkende maatregelen te nemen ten aanzien van de encryptiesoftware. Stichting Digitale Infrastructuur Nederland stelt ook, terecht, dat er geen mogelijkheid bestaat om een achterdeur te introduceren zonder dat het gehele systeem zelf wordt verzwakt.[7] Je moet het naar mijn mening beschouwen als een kaartenhuis: het kan prima overeind blijven staan, maar als je een kaart weghaalt, omdat je wil weten of het een hartenboer of een ruitenboer is, stort het hele huis in.

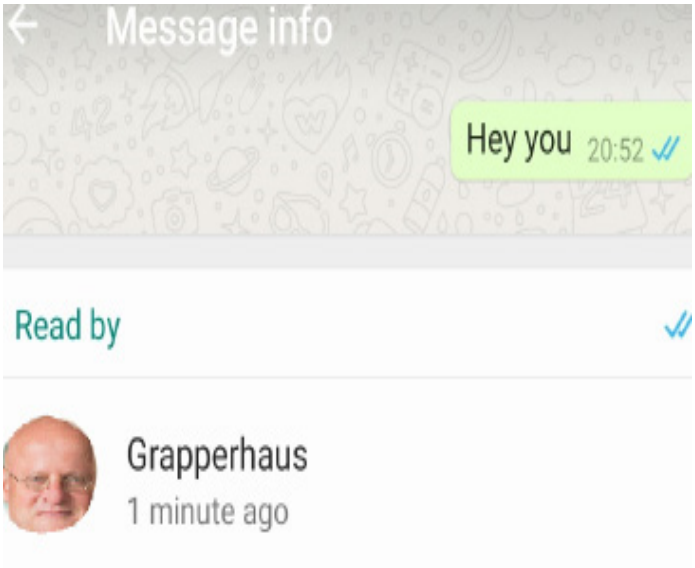
De huidige hackbevoegdheid

Daar komt nog bij dat per 1 maart 2019 de Wet Computercriminaliteit III in werking is getreden met het nieuwe artikel 126nba Sv.[8] Dit nieuwe artikel geeft de overheid de bevoegdheid om geautomatiseerde werken (lees: computers e.d.) binnen te dringen. Met andere woorden, Grapperhaus heeft de bevoegdheid al om in individuele gevallen de telefoons van criminelen te hacken! Ik realiseer mij dat ik geen IT-expert ben, maar er moeten toch genoeg andere manieren zijn om een telefoon binnen te dringen? Als de telefoon immers zelf gehackt kan worden, kunnen dergelijke berichten ook direct gelezen worden. Het hacken van de telefoon zelf is ook niet bepaald gemakkelijk, maar dat is beter te doen dan de chatdiensten zelf. De Amerikaanse FBI kreeg een paar jaar geleden om een soortgelijke kwestie ook al ruzie met Apple.[9] De FBI wilde toegang tot de iPhone van een schutter, die veertien mensen had neergeschoten. Ze vroegen Apple om hulp om de telefoon te ontgrendelen. Apple weigerde dit met dezelfde redenatie, die gebruikt wordt voor E2EE: het is niet te garanderen dat kwaadwillige derden toegang krijgen tot de telefoon via dezelfde methode. De FBI kwam er echter zelfstandig al in, voordat het tot een rechtszaak kwam, dus we hebben jammer genoeg geen definitief antwoord hoe Apple hiermee om had moeten gaan. We kunnen het in ieder geval wel als een mooie vergelijking gebruiken. De overheid kan dan wel zeggen dat ze hulp nodig hebben van de producent met het oog op nationale veiligheid, maar ze zijn prima in staat om er zelf in te komen. En dit zonder dat de beveiliging van de rest van de normale gebruikers wordt geschaad!

Grapperhaus kan daarom maar beter gewoon blij zijn met de mogelijkheden die hij nu heeft en zich hierbij aan het kabinetsbeleid houden. Dat E2EE misbruikt wordt door criminelen, is zorgwekkend en uitermate hinderlijk voor onze opsporingsdiensten. Het maken van een master-key weegt echter niet op tegen de beveiligingslekken die ontstaan voor alle eerlijke burgers, die de chatdiensten gebruiken. Minister Grapperhaus kan daarom beter, in de woorden van dhr. Zenger, “deze keutel intrekken”.[10]

Namens de redactiecommissie,

Bas Smits



7 Wouter Pegtel, “Voorstel meekijkende overheid in versleutelde communicatie volstrekt onacceptabel voor bedrijfsleven”, te vinden op www.dinl.nl (laatst geraadpleegd 1 december 2019).

8 Artikel 126nba Wetboek van Strafvordering, Stb. 2018, 322.

9 Arjan Khupal, “Apple vs FBI: All you need to know”, 29 maart 2016, te vinden op www.cnbc.com (laatst geraadpleegd op 1 december 2019).

10 Rejo Zenger, “Grapperhaus irriteert met gebrek aan kennis over eigen beleid”, 4 november 2019, te vinden op www.bitsoffreedom.nl (laatst geraadpleegd 1 december 2019).

Iedereen is een verdachte

Wat is SyRI?

SyRI staat voor Systeem Risico Indicatie. Het is een systeem van de overheid met als doel om verschillende vormen van fraude, overtredingen en misbruik in verband met belasting of uitkeringen op te sporen door persoonsgegevens van burgers aan elkaar te koppelen. Door middel van technieken van inlichtingendiensten, waaronder datamining en patroonherkenning, wordt alles wat wij als burgers doen in ons dagelijks leven nauwkeurig gevolgd en geanalyseerd. Vervolgens worden met die informatie risicoprofielen van burgers gemaakt. In het verleden werd dit alleen gedaan met al bekende potentiële criminelen, maar nu met SyRI wordt iedereen gezien als een potentieel crimineel.[1]
SyRI wordt formeel het SyRI-besluit genoemd, maar komt van de wet Structuur Uitvoeringsorganisaties Werk en Inkomen van 2013. In het kort, Structuur Uitvoeringsorganisaties Werk en Inkomen (ook wel SUWI) regelt hoe de structuur in verband met de uitvoering van taken inzake de arbeidsvoorziening en de sociale verzekeringswetten is vormgegeven, dus hoe het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Sociale Verzekeringsbank (SVB) en de gemeenten samenwerken als bestuursorganen.[2] SyRI is een onderdeel van de SUWI-wet en is zonder veel berichtgeving aan het algemene publiek als hoofdstuk toegevoegd. Dit gebeurde allemaal al in 2014 en zo trad het SyRI-besluit officieel in werking op 12 september 2014 onder toeziend oog van minister Asscher van Sociale Zaken en Werkgelegenheid (SZW). Zo lijkt het alsof er zonder commentaar of kritiek is gehandeld, maar zowel het College Bescherming Persoonsgegevens als de Raad van State hebben bezwaren gemaakt. Volgens de Raad van State is dit een 'vergaande beperking van de persoonlijke levenssfeer'. Hier is al te zien dat de Raad van State van mening is dat SyRI de Nederlands grondwet schendt (zie verderop).[3] Vervolgens werd ook aangegeven dat de burgers meer informatie zouden moeten verkrijgen over wat er nu precies gebeurt met hun persoonsgegevens. Dit verzoek werd echter niet ingewilligd.

Welke rechten/competenties heeft de overheid aan

1 Bij Voorbaat Bedacht, "Wat is SyRI?", 18 januari 2018, te vinden op www.bijvoorbaatverdacht.nl (laatst geraadpleegd op 1 december 2019).

2 https://www.flexnieuws.nl/caoupdates/wet-structuur-uitvoeringsorganisatie-werk-en-inkomen-suwi.

3 Michael Persson, "Bruger wordt straks doorgelicht zoals profiel van crimineel wordt opgesteld", 1 oktober 2014, te vinden op www.volkskrant.nl (laatst geraadpleegd op 1 december 2019).

SyRI gegeven?

SyrI staat vermeld in artikel 65 van het SUWI-besluit.[4] Een paar punten zijn wel interessant om even bij stil te staan. In lid 1 en 2 worden de grondvoorwaarden voor het gebruik van SyRI vastgesteld: SyRI kan alleen gebruikt worden door de minister op verzoek van een van de organen, zoals is vastgelegd in artikel 64 van het SUWI-besluit met als doel om fraude op te sporen. De minister kan dus niet zelfstandig besluiten om SyRI toe te passen. Het systeem kan verder ook niet gebruikt worden voor andere doeleinden, bijvoorbeeld om andere misdaden op te sporen. Verder wordt in lid 3 gesteld wat de minister met de 'hits' moet doen die uit SyRI voortvloeien. Hij kan ze alleen aan het verzoekende orgaan verstrekken, zolang dit noodzakelijk is bij de uitvoering van hun wettelijke taak. De minister zal dus in elk individueel geval moeten toetsen of de melding die uit SyRI voortvloeit ook relevant is voor het betreffende orgaan. Verder wordt er nog in het artikel gesteld dat de gegevens slechts te gebruiken zijn voor een periode van twee jaar, daarna zullen ze in elk geval verwijderd moeten worden.

De bevoegdheden zijn dus nog in enige mate beperkt. Dit idee krijg je echter niet als je kijkt welke gegevens de minister mag gebruiken hiervoor. SyRI kan volgens het SUWI-besluit namelijk de volgende gegevens aan elkaar koppelen: arbeidsgegevens, boetes en sancties, fiscale gegevens, gegevens over roerende en onroerende goederen, handels-, huisvestings-, identificerende, inburgerings-, nalevings-, onderwijs-, pensioen-, reïntegratie- en schuldenlastgegevens, gegevens over uitkeringen, toeslagen en subsidies en als laatste gegevens over vergunningen en ontheffingen. Dit zijn een hele hoop gegevens, die met eenvoud door het SyRI-systeem kan worden geanalyseerd en gebruikt om een risicoprofiel te creëren van een burger. Deze lijst kan nog worden aangevuld door middel van interpretatie, waardoor ook andere items onder dit artikel zouden kunnen vallen.

De procedure van SyRI

De procedure van SyRI is te verdelen in zeven stappen.[5] Als eerste sluiten twee of meer instanties onder artikel 64 SUWI een zogenoemd samenwerkingsverband en verzoeken tezamen het ministerie van SZW om een risicoanalyse uit te voeren. Als tweede verwerkt de Stichting Inlichtingenbureau, ook wel Informatieknooppunt Gemeenten, de aangeleverde gegevensbestanden volgens de Blackbox-methode. Deze methode gaat als volgt: de bestanden die gekoppeld moeten worden, worden eerst, met een moeilijk woord, gepseudonimiseerd. Vervolgens vindt de koppeling plaats, gevolgd door een analyse. Daar rollen dan de mogelijke fraudegevallen uit, die weer van hun oorspronkelijke naam worden voorzien. Als derde worden de potentiële hits, dus de resultaten die een verhoogd risico laten zien, teruggeleverd aan de Inspectie SZW. Als vierde analyseert de Inspectie SZW de potentiële hits en bepaalt welke gegevens ook daadwerkelijk voor een risicomelding in aanmerking komen. Deze gegevens stuurt de inspectie daarna door naar de belanghebbende instanties, inclusief de politie, of het OM.

Als vijfde zijn de belanghebbende instanties verplicht om verder te onderzoeken of het daadwerkelijk om fraude gaat, voordat ze een sanctie kunnen opleggen. Als zesde worden de risicomeldingen opgenomen in een register dat in eerste instantie niet openbaar is voor het publiek. Dit kan alleen op aanvraag van een burger in worden gezien. Burgers zullen onwetend zijn over het gevoerde onderzoek evenals over de gronden op basis waarvan zij worden ver-

4 Artikel 65 https://wetten.overheid.nl/BWBR0013060/2019-07-08.

5 Bij Voorbaat Bedacht, "Wat is SyRI?", 18 januari 2018, te vinden op www.bijvoorbaatverdacht.nl (laatst geraadpleegd op 1 december 2019).

dacht. Als laatste worden alle resultaten die niet onder een verhoogd risico vallen door het Inlichtingenbureau direct vernietigd. De resultaten die hier wel onder vallen, worden door het ministerie van SZW bewaart voor een maximum van twee jaar.

Bezorgde opinies van deskundigen

Zoals eerder al was genoemd, hadden het College Bescherming Persoonsgegevens en de Raad van State bezwaren gemaakt tegen het SyRI-voorstel, voordat het in werking trad. Er is een niet misplaatste angst dat er misbruik kan worden gemaakt van het systeem, aangezien de gebruikte filtercriteria heel gemakkelijk kunnen worden aangepast. Er kan worden gezocht naar specifieke personen zonder al teveel moeite.[6] Verder gaf de Raad van State ook kritiek op de uitgebreide lijst van gegevens die aan elkaar gekoppeld kunnen worden. Zoals eerder benoemd, kan door interpretatiemethodes een extensieve interpretatie worden gekoppeld aan de in het artikel genoemde items. Zo zei de Raad van State het volgende: 'Er is nauwelijks een persoonsgegeven te bedenken dat niet voor de verwerking in aanmerking komt'. Ook zei de Raad van State het volgende: 'De opsomming lijkt niet bedoeld om in te perken, maar om zoveel mogelijk armslag te hebben'.

Verder heeft ook Philip Alston, VN-rapporteur van de mensenrechten, aangegeven ernstig bezorgd te zijn over Nederland en SyRI. In een aangetekende brief aan de rechtbank in Den Haag vermeldt hij dat het systeem in strijd is met de mensenrechten, omdat het systeem vooral minderheden raakt: mensen met lage inkomens en mensen met een migratieachtergrond, wat in zekere zin een vorm van discriminatie is. Ook zegt hij het volgende: "De privacy van hulpbehoevende burgers lag van oudsher al onder vuur vanwege ingrijpende controles en screenings die ze moesten ondergaan om in aanmerking te komen voor bijstand. Met systemen als SyRI dreigt voor deze burgers echter een technologische surveillancestaat te worden gecreëerd, waarin van het recht op privacy weinig meer dan een illusie overblijft. Men is er tot dusver niet in geslaagd om bedrijven, de overheid en de samenleving in het algemeen ervan te overtuigen dat een verzorgingsstaat, gedreven door technologie, rampzalig zal uitpakken als de inzet ervan niet wordt geleid door respect voor fundamentele rechten."[7] Het is zo dus vrij duidelijk dat Philip Alston tegen het opsporingssysteem SyRI is.

De hiervoor gegeven zorgen zijn gedeeld met de organisatie Bij Voorbaat Verdacht, die, op zijn zachtst gezegd, geen voorstander is van SyRI. Zij heeft met hun juridische team een Wob-verzoek gedaan aan het ministerie over SyRI. Er is niet al te veel nieuwe kennis vrijgegeven, waardoor kan worden geconcludeerd dat het ministerie weigert openheid van zaken te geven.[8]

Is ook Nederland bezorgd over zo'n beveiligingssysteem?

Dit kan heel kort en krachtig worden beantwoord. Het merendeel van de Nederlanders geeft aan 'niks te verbergen' te hebben. Dit is het antwoord dat zij op alles geven inzake van privacyrechten. Het is maar een klein aantal dat zich hier zorgen over maakt. Dit blijkt ook uit het feit dat weinig Nederlanders überhaupt weten dat SyRI bestaat. Er is weinig tot geen commentaar en of bezwaar vanuit de burgers. Reden hiervoor is ook dat er zeer weinig informatie openbaar is gemaakt over het systeem en in hoeverre het de privacy van een burger aantast. Daarentegen groeit de zorg

6 Michael Persson, "Bruger wordt straks doorgelicht zoals profiel van crimineel wordt opgesteld", 1 oktober 2014, te vinden op www.volkskrant.nl (laatst geraadpleegd op 1 december 2019).

7 Nieuwsuur, "VN-rapporteur zeer bezorgd over Nederlandse opsporingssysteem voor uitkeringsfraude", 21 oktober 2019, te vinden op www.nos.nl (laatst geraadpleegd op 1 december 2019).

8 Bij Voorbaat Verdacht, "wat u niet mag weten over hoe SyRI u profileert", 15 februari 2018, te vinden op www.bijvoorbaatverdacht.nl (laatst geraadpleegd op 1 december 2019).

over privacy wel. Uit een onderzoek van Ruigrok NetPanel blijkt dat de zorgen over de online veiligheid van persoonlijke gegevens is toegenomen en dat 52 procent van de Nederlanders bezorgd tot zeer bezorgd is.[9] Dit gaat van het onderwerp af, omdat het vooral gaat om zorgen dat derden, waaronder bedrijven en criminelen misbruik kunnen maken van persoonlijke gegevens. Alleen wordt vaak vergeten dat ook de overheid gegevens wil verzamelen van zijn burgers.

Toekomst: naar een utopie of dystopie?

Het opsporingssysteem SyRI kan ervoor zorgen dat mensen die misbruik maken van de gulheid van Nederland sneller en beter kunnen worden aangepakt. Zo zou, in theorie, het geld dat hiermee wordt teruggewonnen, kunnen worden geleverd aan diegenen die ook daadwerkelijk financiële ondersteuning nodig hebben. Als deze theorie zich ook zo uitwerkt, kan men het zien als een goede stap in de richting van een utopie (althans als men socialisme een item vindt van een utopie). Daarentegen kan men zich afvragen of we hiermee een soort Big Brother-wereld creëren. Het SyRI-systeem kan de eerste stap zijn in de richting van een wereld, waarin alles wordt bekeken en gecontroleerd door de overheid. Zijn we als een samenleving bereid om in zoverre onze vrijheid op te geven voor een socialistisch ideaal?

Namens de redactiecommissie,

Caitlin Verhoeven

9 CustomerTalk, "De online privacy is nog steeds een issue voor Nederlanders", 25 juni 2019, te vinden op www.customertalk.nl (laatst geraadpleeg op 1 december 2019).