Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 926 Initiatiefnota van het lid Koopmans: Onderlinge privacy

Nr. 2

INITIATIEFNOTA

1. Het Probleem: belang en bedreiging van de onderlinge privacy

Online shaming, sextortion en internetpesten zijn aan de orde van de dag. Beelden zijn vaak voor eeuwig en kunnen wereldwijd worden gedeeld. Met gezichtsherkenningstechnologie, die nu ook voor privépersonen beschikbaar is, is straks niemand meer anoniem op straat. Een mobiele telefoon is ook een camera die wereldwijd kan uitzenden, ook zonder dat de gefilmde het weet. Verborgen camera's en afluisterapparatuur zijn niet alleen van de AIVD maar van iedereen. Met simpele locatie-trackers, microfoons en drones kan iedereen ongezien worden gevolgd, ieder gesprek worden opgenomen en ieder hoekje worden gefilmd. Door data-profilering en tracking-technologie is het privéleven van iedereen heel makkelijk in kaart te brengen, ook door medeburgers en kleine bedrijven.

De situatie is fundamenteel anders dan vroeger. Er is een groot verschil tussen de buurman die tussen de schutting door *gluurt* en de buurman die tussen de schutting door *filmt*, want films zijn terug te zien, kunnen met iedereen worden gedeeld en gekoppeld aan andere persoonlijke informatie. Informatie-technologie heeft grote consequenties voor de manier waarop we leven.[1] Naast de vele en belangrijke positieve gevolgen van efficiëntie, handel, verbondenheid en informatieverschaffing staan ook belangrijke negatieve aspecten zoals permanente observatie en individuele analyse. Dit kan gevolgen hebben voor hoe vrij mensen zich voelen, en soms ook voor hoe veilig ze daadwerkelijk zijn.

Kan je nog wel vrij en veilig leven als alles wat je doet en zegt door iedereen zonder jouw medeweten en zonder jouw instemming kan worden opgenomen en gepubliceerd? Durf je dan nog wel een vertrouwelijk gesprek te voeren, eerlijk je mening te geven, met of zonder bikini in de tuin te zitten, of gewoon «gek» te doen? De mogelijkheden van sociale controle worden bijna onbeperkt, zonder vergetelheid en vaak zonder vergiffenis. Dit grijpt nu al diep in het leven van mensen in.

[1] Zie verder hierover het rondetafelgesprek dat de Vaste Kamercommissie voor Justitie en Veiligheid organiseerde op 7 december 2017.

kst-34926-2
ISSN 0921 - 7371
's-Gravenhage 2018

Allochtone meisjes worden heel vaak «exposed» als ze zich «westers» gedragen.[2] Stiekem gemaakte seksfilmpjes ruïneren levens. Beeldchantage neemt toe, jongeren plegen zelfmoord.[3] Deze ontwikkeling is politiek belangrijk. Zonder privacy bestaat immers geen vrijheid. Daarom is de huidige privacy-discussie te beperkt.

De huidige privacy-discussie blijft grotendeels beperkt tot de vraag wat de staat – en nu ook grote bedrijven – van mensen mogen weten: hoe beschermen we mensen voor Orwell's *Big Brother*? Zeker, voor de vrijheid van het individu moeten machtige actoren goed gereguleerd worden. Deze «verticale privacy» wordt beschermd door onder meer art. 10 Grondwet, art. 8 EVRM en de Algemene Verordening Gegevensbescherming. Maar in de moderne tijd hebben ook burgers zelf veel mogelijkheden om elkaars privacy te schenden, bewust en onbewust, kwaadwillend of goedwillend. Zo kunnen ze elkaars vrijheid afnemen. De privacy tussen burgers onderling, de «horizontale privacy» of «onderlinge privacy», moet dus ook goed gereguleerd worden. Hoe beschermen we onszelf tegen het gluren, de sociale controle, de betutteling en de morele dwang van miljoenen *Little Brothers*?

Het Regeerakkoord stelt dat de regering zich zal inzetten voor de betere bescherming van de privacy tussen burgers onderling. Een onderdeel van dit beleid zal zijn het als apart delict strafbaar stellen van wraakporno. Maar onderlinge privacy omvat nog zo veel meer. Problemen bestaan niet alleen in de omschrijving van rechten, maar ook in de praktijk van preventie, handhaving en vervolging. Op veel terreinen kunnen burgers, bedrijven en overheid goed samenwerken. Dit alles zonder enige beperkingen te willen introduceren in de huidige dagelijkse praktijk waarin veel mensen, bijvoorbeeld op Facebook, allerlei informatie over zichzelf willen delen voor sociale of economische doeleinden. Weg met betutteling, of die nu van de overheid komt of van andere burgers. De persoonlijke vrijheid en de eigen verantwoordelijkheid staan voorop.

2. Tegenwerpingen

Tegenstanders van regulering van onderlinge privacy gebruiken diverse argumenten. Een eerste is de eigen verantwoordelijkheid: iedereen moet zich gewoon gedragen en zelf opletten. Veel mensen zetten hun privéleven op Instagram: zij mogen dan niet klagen dat dat bekend wordt. Zeker, er is een grote eigen verantwoordelijkheid voor het beveiligen en al dan niet verspreiden van compromitterende beelden en gegevens. Maar nu het zo eenvoudig is geworden om andermans privacy te schenden, is een verwijzing naar de eigen verantwoordelijkheid van het slachtoffer minder geloofwaardig. Natuurlijk, over wat je zelf publiceert mag je niet klagen, maar van wat anderen stiekem van jou filmen heb je geen weet. Daarnaast zijn veel privacy-problemen niet zelfstandig te vermijden. Niemand kan zich verschuilen voor verborgen camera's, data-profilering en gezichtsherkennings-software.

Een andere tegenwerping is dat het nog te vroeg is: veel technologie is nog in ontwikkeling, privacy-schendingen hebben de samenleving nog niet ontwricht. Dit gaat er aan voorbij dat er al veel gevallen zijn waarin

---

[2] https://nos.nl/op3/artikel/2207855-vrouwen-online-exposed-bangalijsten-zijn-hierbij-kinderspel.html (16 december 2017).

[3] In 2017 pleegde de 14-jarige Onur uit Enschede zelfmoord na publicatie van een naaktfoto. Een Nederlander is veroordeeld voor het afpersen van tientallen meisjes en het tot zelfmoord drijven van de Canadese Amanda Todd. In 2016 werd 851 keer melding gemaakt van bedreiging of chantage met een foto of een video. In 266 gemelde gevallen stonden er naaktfoto's en video's online (Kamerbrief Minister van J&V 24 november 2017).

levens zijn geruïneerd door bijvoorbeeld online *shaming*, stiekeme opnames en wraakporno. Ook miskent dit argument de sterke sociale controle die nu al uitgaat van het gebruik van technologie, zoals bijvoorbeeld bij het «exposen» van allochtone vrouwen. Veel mensen denken nu al twee keer na voordat ze iets «geks» doen, omdat het altijd ongemerkt opgenomen kan worden. En voor zover nu nog mogelijk is het beter om te anticiperen op problemen dan om ze eerst groot te laten worden.

Een volgende tegenwerping is dat het al te laat is: de technologie bestaat al en kan niet meer worden verboden. Inderdaad, veel ontwikkelingen zijn onomkeerbaar. Maar dat betekent niet dat er geen ruimte meer is voor beleid en regulering. Vaak zal dat alleen kunnen in samenwerking met de industrie en in internationaal verband. Maar ook in Nederland kan op belangrijke terreinen effectief worden opgetreden. Er is geen reden voor defaitisme.

Een laatste tegenwerping is dat de moderne samenleving zal leren leven met de afwezigheid van privacy en dat de moraal zich hieraan zal aanpassen. Zeker, hopelijk zullen technologische ontwikkelingen zoals gezichtsherkenning en de alomtegenwoordigheid en miniaturisering van camera's en microfoons een goede plaats vinden in de maatschappij. Maar in Nederland houdt iedereen het recht op bescherming van zijn persoonlijke levenssfeer. Uitvinders en technologie hebben geen *carte blanche* om dat grondwettelijke recht te beperken. Een vrije samenleving moet ruimte blijven bieden voor vertrouwelijkheid, vergissingen en het recht met rust gelaten te worden. Dat vereist optreden, zonder technofobie, zonder technofilie, en zonder taboes.

3. De Stand van Zaken

- Bij een evidente inbreuk op intellectueel eigendom is er een spoedprocedure (art. 1019(e) van het Wetboek van Burgerlijke Rechtsvordering) om bij rechterlijk bevel de inbreuk te verbieden, zo nodig ook zonder dat de dader bekend is, en de resultaten onmiddellijk te verwijderen. Ook kunnen internetproviders worden bevolen maatregelen te treffen en zijn inbreukmakers verplicht de herkomst en verspreiding van materiaal op te geven. Bij eenzelfde evidente inbreuk op privacy geldt dat niet.
- Art. 139(f) Wetboek van Strafrecht verbiedt het geheim filmen van mensen op niet-publieke plaatsen. Vervolging is sporadisch en straffen zijn laag. Het stiekem opnemen van een privégesprek is bij wet toegestaan.
- Per 25 mei 2018 treedt de EU-verordening over de verwerking van persoonsgegevens (AVG) in werking. Zij harmoniseert met name de privacyregels van burgers jegens overheid en bedrijven, de «verticale privacy». De Nederlandse Autoriteit Persoonsgegevens (AP) is toezichthouder. Zij heeft ook het mandaat toe te zien op schendingen door burgers onderling, maar doet hier vooralsnog nauwelijks iets mee.
- De AVG reguleert ook het «recht op vergetelheid». Ieder databedrijf hanteert andere methodes om dit recht vorm te geven.
- Spionagesoftware wordt door private partijen ingezet tegen burgers en bedrijven. De (vorige) Minister erkende dat deze software makkelijk verkrijgbaar is, maar dat voor veel producten relevante regelgeving ontbreekt.[4]

[4] Antwoorden van de Minister van V&J op mijn Kamervragen van 7 april 2017, d.d. 24 mei 2017.

- Ondanks een verbod op *reclame* voor verborgen camera's is de verkoop ervan ongelimiteerd.[5] Daarenboven mogen zowel zichtbare als onzichtbare camera's overal zonder beperking worden opgehangen, zolang ze in bepaalde gevallen maar niet worden gebruikt.[6] Of ze daadwerkelijk niet gebruikt worden is niet te controleren. Handhaving is uiterst summier dan wel afwezig.
- Er zijn in Nederland geen specifieke privacyregels voor de inzet van hobbydrones,[7] in veel andere landen wel. De bestuurder van een hobbydrone kan op afstand, anoniem en vaak ontraceerbaar filmen. Hobbydrones kunnen daarnaast onherkenbaar zijn. Fysieke handhaving is vaak onmogelijk vanwege de afwezigheid van anti-drone middelen.
- Zelfs na uitgezonden verkrachtingen is het heel moeilijk om verspreiders aan te pakken, en bijna onmogelijk om beelden te verwijderen. Slachtoffers van evidente privacy-schendingen moeten vaak zelf civiele procedures financieren, terwijl daders niet of nauwelijks worden beboet. Strafrechtelijke vervolging vindt nauwelijks plaats.
  - De 17-jarige Chantal moest meerdere processen voeren om de politie, Facebook en haar school te dwingen haar te helpen de dader van wraakporno te achterhalen, nu nog steeds zonder resultaat.
  - Nikki Lee Janssen, slachtoffer van een hack van privéfilmpjes waarmee ze werd gechanteerd, moest drie keer aangifte doen en werd voor 1 miljoen mensen op Dumpert te kijk gezet.[8] In een civiele procedure werd het door Dumpert bewust blijven publiceren van haar beelden wel onrechtmatig geacht, maar behalve het afdragen van de advertentie-inkomsten volgde geen enkele vorm van boete of straf.[9]
- De politie zegt zelf te weinig kennis over onderlinge privacy-schendingen te hebben.[10]
- Met al bestaande software, geplaats in een smartphone of bril, kan je een onbekende automatisch herkennen. Door eenvoudige koppeling van bestanden (illegaal, maar niet te handhaven) is iedereen identificeerbaar als bijvoorbeeld homo, politiek betrokken of al dan niet kredietwaardig.

4. Beslispunt

De indiener vraagt de Kamer in te stemmen met het verzoek aan de Minister voor Rechtsbescherming, in samenspraak met zijn collega's van andere departementen, een ambtelijke taskforce Onderlinge Privacy op te richten die met als einddatum 1 december 2018 werk maakt van c.q. onderzoek doet naar de volgende deeloplossingen:

Rechtsbescherming

a) Slachtoffers van evidente en ernstige privacy-schendingen (zoals het douche-filmpje van de NL handbalsters) een vergelijkbare rechterlijke spoedprocedure met *ex parte*-bevelen bieden als slachtoffers van

---

[5] Antwoorden van de Minister van V&J op mijn Kamervragen van 8 augustus 2017, d.d. 14 september 2017.

[6] Antwoorden van de Minister van V&J op mijn Kamervragen samen met het Lid Bruins Slot (CDA) van 7 juli 2017, d.d. 4 september 2017.

[7] Antwoorden van de Minister voor Rechtsbescherming op mijn Kamervragen van 25 oktober 2017, d.d. 27 november 2017.

[8] Antwoorden van de Minister van V&J op mijn Kamervragen samen met het Lid Tellegen (VVD) van 4 juli 2017, d.d. 6 september 2017.

[9] Rb Amsterdam, 2 februari 2018 (Janssen/GS Media B.V.)

[10] Rondetafelgesprek van de Vaste Kamercommissie voor Justitie en Veiligheid, 7 december 2017.

inbreuken op intellectuele eigendomsrechten die nu hebben conform art. 1019 (e) Wetboek van Rechtsvordering.
b) Faciliteren van online aangifte bij onderlinge privacy-schendingen.
c) Vergroten van de kennis over onderlinge privacy bij politie, OM en rechterlijke macht.
d) Versterken van het al bestaande recht op vergetelheid door het doen van aangifte mee te laten wegen als factor in het door internetplatforms urgent honoreren van een verzoek tot verwijdering, expliciet zonder daarbij bijvoorbeeld fraudeurs te beschermen. [Bijv. nuttig in het geval van het douche-filmpje van de NL handbalsters]
e) Bij de uitwerking van de voorgenomen Europese standaarden voor Internet of Things apparaten samen met het bedrijfsleven bijzondere aandacht te geven aan de privacy-risico's van producten die een aanzienlijk privacy-risico kennen, zoals spraakconsoles in huis en met het internet verbonden auto's.
f) Brede strafbaarstelling van wraakporno, waaronder begrepen het delen en/of publiceren van intieme beelden waarmee het vertrouwen van het slachtoffer wordt geschaad.
g) Het verbeteren van hulp aan slachtoffers van evidente ernstige privacy-schendingen, inclusief het strafrechtelijk vervolgen van bewuste verspreiders van deze inbreuken, en het evalueren van de huidige strafmaat, nu momenteel te vaak wordt volstaan met verwijdering van de beelden, zonder bijkomende straf.

Rechtsversterking

h) Onderzoeken van een mogelijk vergunningenstelsel voor de verkoop van specifiek voor spionage bedoelde producten zoals spy-camera's en spionagesoftware.
i) Onderzoek naar reguleren van het privégebruik van gezichtsherkennings-technologie.
j) Onderzoek naar praktische waarborgen tegen de privacy-risico's van hobbydrones.
k) Samen met het bedrijfsleven standaard-protocollen voor vergetelheidsverzoeken ontwikkelen. Dit zonder aantasting van de vrije meningsuiting, de persvrijheid en zonder onbedoeld ook bijvoorbeeld fraudeurs te beschermen.
l) Voorstellen ontwikkelen voor het niet langer toestaan van het stiekem opnemen van privégesprekken, behoudens evident publiek belang zoals onderzoeksjournalistiek.

Informatie en samenwerking

m) Vergroten van het maatschappelijk bewustzijn over de eigen verantwoordelijkheid bij privacybescherming.
n) Europese en internationale samenwerking ter versterking van de onderlinge privacy.
o) Onderzoeken van de onderlinge privacybescherming in het buitenland, waaronder het Duitse grondrecht van «Informationelle Selbstbestimmung».
p) Het nauwgezet en stelselmatig betrekken van mensen, bedrijven en organisaties uit de praktijk, al dan niet in de vorm van een nationaal onderling-privacy-samenwerkingsverband, voor het adviseren van de taskforce Onderlinge Privacy en het ontwikkelen van ideeën, monitoren van ontwikkelingen, het agenderen van onderlinge privacy-onderwerpen en het bevorderen van een praktische discussie over de bescherming van de persoonlijke levenssfeer tussen mensen onderling.

5. Financiële paragraaf

Het oprichten van een ambtelijke taskforce Onderlinge Privacy kan binnen de huidige begroting. Voor de voorgestelde onderzoeken kan gebruik worden gemaakt van de bestaande kennisinfrastructuur zoals het WODC en het Rathenau Instituut. Er zijn geen nieuwe kosten gemoeid met de beoogde samenwerking met bedrijfsleven en burgerorganisaties. De inventarisatie van onderlinge privacybescherming in het buitenland, alsook het agenderen van onderlinge privacy in Europees verband kan met het bestaande apparaat. Kennisvergroting in de justitiële keten zal beperkte financiële gevolgen kunnen hebben, die afhankelijk zullen zijn van de wijze van invulling, zoals uit te werken door een ambtelijke taskforce Onderlinge Privacy.

Koopmans