Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat-Generaal Rechtspleging en Rechtshandhaving

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
T 070 370 71 43
F 070 370 79 00

Ons kenmerk
2600162

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 7 juni 2019
Onderwerp Bescherming van de horizontale privacy

1. Inleiding

Technologie biedt geweldige kansen. De ontwikkelingen rond gezichts- en spraakherkenning, big data, geïntegreerde algoritmes en de steeds verdergaande koppeling van apparaten via het internet (‘internet of things’) zorgen voor nieuwe applicaties die ons leven op tal van punten vergemakkelijken. Tegelijkertijd confronteren die ontwikkelingen ons ook met nieuwe risico’s. Door het toenemende gebruik en de koppeling van persoonlijke data, wordt het risico dat de privacy van individuele personen in het geding komt groter.

Tegen die achtergrond stelt het kabinet zich als doel dat burgers zich vrij en veilig voelen in een digitaliserende wereld. Om dit doel te bereiken moeten burgers, bedrijven en instellingen zich meer bewust worden van de risico’s op het gebied van privacy, zodat ze daar zelf beter rekening mee kunnen houden. Waar de privacy in het gedrang komt, moeten mensen meer mogelijkheden hebben om daar tegen op te treden. En waar nodig worden de normen voor privacybescherming door de overheid versterkt.

In deze brief staat de bescherming van horizontale privacy centraal.[1] Dit sluit aan bij de ambitie van het kabinet om in te zetten op het beschermen van de privacy van burgers onderling.[2]

Met horizontale privacy wordt gedoeld op de privacy tussen burgers onderling en tussen burgers en bedrijven. Zij onderscheidt zich daarmee van de verticale privacy, die betrekking heeft op de relatie burger-overheid. De focus op de horizontale privacy betekent niet dat technologische ontwikkelingen niet ook gevolgen kunnen hebben voor de verticale privacy. Integendeel, die gevolgen

[1] Andere redenen om technologische ontwikkelingen in goede banen te leiden, zijn onder meer gelegen in publieke waarden als veiligheid, zelfbeschikking en solidariteit. Aandacht voor deze waarden in relatie tot die ontwikkelingen wordt onder meer gegeven in de Nederlandse Digitaliseringsstrategie (Kamerstukken II 2017/18, 26643, nr. 541).
[2] Vertrouwen in de toekomst. Regeerakkoord 2017–2021, p. 6.

krijgen dan ook aandacht in andere trajecten.[3] De horizontale privacy is daarentegen een onderwerp dat onderbelicht is, terwijl de voortschrijding van de techniek wel om meer aandacht daarvoor vraagt.

Tegen die achtergrond heb ik toegezegd met een kabinetsvisie op de bescherming van horizontale privacy te komen.[4] Met deze brief doe ik mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties deze toezegging gestand. In overeenstemming met de motie-Rutte[5] besteed ik in een bijlage bij deze brief ook aandacht aan de initiatiefnota 'Onderlinge privacy' van het lid van uw Kamer Koopmans.[6]

2. Wat is het belang van bescherming van de horizontale privacy?

Het is mensen eigen om zich vrij en veilig te willen voelen en zich te gedragen zoals ze willen. Zich vrij en veilig te voelen in de informatie die zij delen, in de relaties die zij met anderen aangaan, in de wijze waarop met hun lichaam wordt omgegaan en in de wijze waarop zij zich binnen de eigen woning, maar ook daarbuiten gedragen. Het kabinet acht deze vrijheid en veiligheid essentieel om mensen zich te kunnen laten ontwikkelen, zoals zij zelf willen. Alleen in vrijheid kunnen mensen ten volle hun persoonlijke identiteit ontwikkelen. Met andere woorden: mensen behoeven een persoonlijke levenssfeer of 'privacy' om dit te bereiken.

Privacy is naar het oordeel van het kabinet niet alleen van belang voor ieder mens afzonderlijk, maar ook voor de samenleving als geheel. De persoonlijke identiteit van mensen is belangrijk voor het ontwikkelen van een zelfstandig en sociaal actief burgerschap, dat op haar beurt weer de basis vormt voor een goed functionerende democratische rechtsstaat. De behoefte aan privacy vertaalt zich bovendien in sociale normen als het tonen van respect voor andermans levenssfeer. Dat is nodig voor een samenleving waarin burgers zich in harmonie met elkaar kunnen gedragen en ontwikkelen.

Het belang van privacy impliceert dat deze goed wordt beschermd. Dit belang is zo groot dat de bescherming daarvan een fundamenteel recht van ieder mens is, een grondrecht dat verankerd is in verschillende verdragen, in regelgeving van de Europese Unie, in onze Grondwet en in verscheidene wetten.

Het recht op privacy is een belangrijk grondrecht, maar is niet onbegrensd. Het recht op privacy van de ene burger kan op gespannen voet staan met een grondrecht van een andere burger. In dat geval moet de wetgever of de rechter zo nodig een afweging tussen beide rechten maken. Zo krijgt een journalist in het kader van de vrijheid van meningsuiting van de rechter in het algemeen veel ruimte om zijn werk te doen, ook als daardoor de privacy van personen over wie hij schrijft, in het geding is.

3. Technologische ontwikkelingen: kansen en risico's voor de privacy

[3] Voorbeelden hiervan zijn de trajecten rond het vastleggen en bewaren van kentekengegevens door de politie ('ANPR') en de Wet computercriminaliteit III. Zie verder bijvoorbeeld de brief van oktober 2018 over transparantie van algoritmes bij de overheid (Kamerstukken II 2018/19, 26643, nr. 570).
[4] Handelingen II 2017/18, 29, item 3, p 29.
[5] Kamerstukken II 2017/18, 34926, nr. 4.
[6] Kamerstukken II 2017/18, 34926, nr. 2.

3.1 Kansen

De bescherming van de privacy vergt voortdurend onderhoud. Techniek kan daarbij helpen. Zo werd al aan het eind van de vorige eeuw het belang van *Privacy Enhancing Technologies* als pseudonimisering en encryptie erkend. Deze technieken hebben inmiddels een aanzienlijke bijdrage aan de bescherming van persoonsgegevens geleverd.

Denk verder aan computerprogramma's waarmee privacyverklaringen van bedrijven met behulp van *machine learning* volledig geautomatiseerd kunnen worden geëvalueerd op de mate van naleving van de Algemene verordening gegevensbescherming (AVG). Zo'n programma kan bedrijven helpen hun privacyverklaringen te verbeteren, mensen ondersteunen bij het opkomen voor hun belangen en zowel consumentenorganisaties als toezichthouders eventueel aanzetten tot actie.[7]

Een ander voorbeeld is de ontwikkeling van zoekmachines die de privacy zoveel mogelijk beschermen. Zoals Startpage.com, een zoekmachine die geen persoonlijke data opslaat, geen gebruikersprofielen opbouwt en met behulp van 'anonieme weergave' voorkomt dat je bekend raakt bij een website die je bezoekt.[8]

Het kabinet juicht dit soort ontwikkelingen toe. Niet alleen kunnen zij bijdragen aan bescherming van de privacy, maar zij laten ook goed zien dat technologische ontwikkelingen met betrekking tot dit terrein niet alleen risico's, maar ook kansen bieden.

3.2 Risico's

Technologische ontwikkelingen brengen voor de bescherming van de privacy als gezegd ook risico's mee. Er zijn steeds meer manieren om persoonsgegevens te genereren, deze op te slaan en verder te verspreiden. De verwerking van dergelijke gegevens voor commerciële doeleinden is daardoor enorm gegroeid. Mensen weten vaak niet welke gegevens over hen worden verwerkt en met welk doel. Zij komen er meestal pas achter nadat op basis van een profiel een beslissing is genomen die hen in hun belang raakt, zoals het weigeren van een lening, verzekering of abonnement. Een ander risico is dat sommige gegevens of opgestelde profielen onjuist zijn, met mogelijk verstrekkende gevolgen voor mensen. Mensen verliezen op deze wijze steeds meer het overzicht en de zeggenschap over hun gegevens en daarmee over de keuzes in hun leven.[9]

Bij grote techbedrijven die een dominante positie innemen, speelt bovendien dat zij deze positie kunnen gebruiken om minder bescherming van persoonsgegevens te bieden, met name wanneer dataverzameling een belangrijk onderdeel van het verdienmodel vormt. Gebruikers hebben dan geen alternatieve aanbieder om naar

---

[7] Zie: CLAUDETTE meets GDPR Automating the Evaluation of Privacy Policies using Artificial Intelligence 2018, http://www.claudette.eu/gdpr/#, en Hamza Harkous c.s., Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning,https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.

[8] Zie: https://www.startpage.com. Deze zoekmachine won de Nederlandse Privacy Award 2019.

[9] Zie ook: Toezichtkader Autoriteit persoonsgegevens. Uitgangspunten voor toezicht 2018-2019, p. 8.

over te stappen als zij de gegevensbescherming die het dominante bedrijf biedt, te gering vinden.

Risico's voor de bescherming van de privacy doen zich niet alleen in de relatie tussen burgers en bedrijven voor. Zij doen zich ook voor in de relatie tussen burgers onderling. Denk aan het gebruik van internet voor *naming and shaming* of het plaatsen van (seksueel) beeldmateriaal om de afgebeelde persoon in een compromitterende situatie te brengen. Of aan het gebruik van gezichtsherkenning om *facial profiles* aan te maken waarmee bijvoorbeeld mensen met een hoog IQ, witte-boorden-criminelen of terroristen zouden kunnen worden gedetecteerd.[10]

Verder zien we een toenemend gebruik van camera's op smartphones om verkeersslachtoffers en andere personen in hulpbehoevende toestand te fotograferen of te filmen. Ook worden soms zeer kleine, verborgen camera's gebruikt om intieme beelden te maken[11] of camera's aan drones waarmee mensen worden gefilmd op plaatsen waar zij dat niet verwachten. Een techniek die onze privacy ook kan raken, is locatietracking, waarmee kan worden vastgelegd wat bijvoorbeeld de gebruiker van een smartphone dagelijks doet. Dat kunnen activiteiten zijn waarvan die persoon liever niet wil dat die bij anderen bekend worden. De combinatie van technieken kan de risico's nog groter maken: opnamen met een 'spycamera' die met behulp van gezichtsherkenning en locatietracking aan namen en plaatsen worden gekoppeld en vervolgens op internet worden verspreid.

Risico's voor de privacy doen zich ook voor bij de opmars van 'internet of things' (IoT), het verschijnsel dat allerlei apparaten en andere voorwerpen, variërend van smart-TV's tot speelgoedpoppen en spraakconsoles, met internet zijn verbonden. Zo wees onderzoek uit dat bepaald speelgoed kan worden gebruikt om gesprekken af te luisteren en kinderen met gerichte reclame te bestoken.[12]

Met betrekking tot DNA zien we – tot slot - dat commerciële analysebureaus in opkomst zijn die aan de hand van DNA kunnen helpen nieuwe familieleden te vinden en etnische oorsprong te ontdekken, maar ook om informatie te krijgen over genetische aanleg voor verschillende aandoeningen.[13] Het feit dat het hierbij om zeer gevoelige gegevens kan gaan, zoals informatie over een verhoogde kans op bepaalde erfelijke ziektes, verhoogt het risico van een inbreuk op de privacy van niet alleen de aanvrager, maar ook die van zijn verwanten.

4. Rollen en verantwoordelijkheden

Privacy gaat ons allemaal aan. En ook de taak om die privacy te beschermen komt ons allemaal toe. Individuele burgers hebben daar zelf een belangrijk aandeel in. Bedrijven hebben een verantwoordelijkheid om zorgvuldig met gegevens om te gaan. En de overheid speelt een normerende en handhavende rol.

---

[10] Zie bijvoorbeeld: https://www.faception.com/.

[11] Denk aan zgn. *upskirt*-camera's, die op schoenen zijn bevestigd en waarmee vrouwen onder hun rok worden gefilmd. Zie: https://www.msn.com/nl-nl/nieuws/binnenland/gluurbeelden-honderden-nederlandse-vrouwen-gedeeld-in-online-netwerk/ar-AAAtIFC.

[12] https://www.mijnonlineidentiteit.nl/internet-of-toys-privacy-veiligheid/.

[13] Zie bijvoorbeeld: https://www.myheritage.nl/, https://www.igene.nl/ en https://www.23andme.com/.

4.1 Rol en verantwoordelijkheid van de burger

In een samenleving waarin technologische ontwikkelingen een toenemend risico van schending van de privacy meebrengen, is meer dan ooit van belang dat burgers de privacy van hun medeburgers respecteren. Nu het door deze ontwikkelingen steeds gemakkelijker wordt om alles van iedereen te weten te komen, is het des te belangrijker dat burgers zich beperken in wat zij van anderen willen weten. Omgekeerd geldt dat zij niet willen dat anderen alles van hen weten. Het gaat hier bovenal om een sociale norm, die eraan bijdraagt dat mensen in harmonie met elkaar kunnen leven.

Van belang is verder dat het tussen burgers onderling om verschillende typen relaties kan gaan: werkgever-werknemer, ouder-kind enz. Al deze relaties kennen hun eigen machts- en sociale verhoudingen met als gevolg verschillen in de sociale en juridische normen die van toepassing zijn. Hetzelfde geldt met betrekking tot de relatie die burgers tot bedrijven en overheden hebben.

Welk type relatie het ook betreft, burgers hebben ook een rol en verantwoordelijkheid in het beschermen van hun eigen privacy. Die verantwoordelijkheid begint al met na te denken over welke gegevens je wel of niet wil delen. Verder kan iemand zijn persoonsgegevens beschermen door gebruik te maken van de rechten die de AVG hem daartoe geeft, zoals het recht op inzage, op correctie en op vergetelheid.[14] Ook kan hij bij een overtreding van de AVG eventueel een klacht bij de Autoriteit persoonsgegevens indienen. Daarnaast kan hij een beroep doen op het civiele recht om zijn privacy te beschermen of kan hij bij een eventuele strafrechtelijke overtreding van een privacynorm aangifte doen bij de politie.

4.2 Rol en verantwoordelijkheid van het bedrijfsleven

Ook voor bedrijven geldt dat zij de privacy van burgers moeten respecteren. De sociale norm is hier die van verantwoord ondernemerschap, die kan bijdragen aan een bestendige, langdurige relatie met hun klanten.

Verder geldt ook hier dat de relatie tussen een bedrijf en een burger kan verschillen. Tussen een kleine winkelier die in een vertrouwde, persoonlijke relatie tot zijn klanten uit de wijk staat en een groot techbedrijf dat met data van miljoenen burgers in een onpersoonlijke en daarmee niet op voorhand vertrouwde relatie tot die burgers staat, bestaat een groot verschil.

Het bedrijfsleven kan bij de bescherming van de privacy een belangrijke rol vervullen met onder meer het instrument van zelfregulering, zoals gedragscodes, certificering en bindende bedrijfsvoorschriften.[15] Voor een praktische invulling van voorschriften uit de AVG kan verder worden gedacht aan het opstellen van privacyverklaringen of het ontwikkelen van dashboards waarop betrokken consumenten hun privacy-instellingen kunnen aanpassen.

4.3 Rol en verantwoordelijkheid van de overheid

Grondrechten verplichten de overheid geen inbreuken te maken op de rechten van burgers. Grondrechten kunnen ook een positieve verplichting voor de overheid met zich brengen: om ervoor te zorgen dat de grondrechten effectief

[14] Zie de artikelen 15, 16 en 17 AVG.

[15] Zie de regeling daarvan in artikel 40 tot en met 43 en 47 AVG.

gerespecteerd worden, is actief handelen van de overheid nodig om een recht daadwerkelijk te realiseren. De overheid moet zich dus niet alleen onthouden van inbreuken op iemands privé-, familie- en gezinsleven, maar in bepaalde gevallen moet de overheid actief optreden om te zorgen dat een (rechts)persoon geen inbreuk maakt op het grondrecht van de andere persoon. Zij vult deze taak in met voorlichting, onderwijs, wetgeving, toezicht en handhaving.

De voorlichtende rol van de overheid met betrekking tot de AVG ligt primair bij de Autoriteit persoonsgegevens (AP). Daarnaast zijn er ministeries die specifiek op hun terrein voorlichting over geven de AVG.

Bescherming van de privacy vergt ook aandacht in het onderwijs. In het huidige onderwijscurriculum wordt vooral onder de noemers 'sociale veiligheid', 'mediawijsheid' en 'Informatiebeveiliging en privacy (IBP)' aandacht besteed aan privacybewustzijn op school en de ontwikkeling van privacyvaardigheden van leerlingen.

Het instrument van wetgeving komt in beeld bij: 1) het verbieden van gedragingen die een schending van de privacy opleveren (zoals het heimelijk filmen van mensen), 2) het verschaffen van rechten aan mensen om hun privacy te kunnen beschermen (zoals het recht om hun persoonsgegevens in te zien) en 3) het opleggen van verplichtingen aan personen en organisaties om de privacy te beschermen (zoals de verplichting om betrokkenen te informeren over het feit dat hun persoonsgegevens worden verwerkt).

Het toezicht op naleving van voorschriften uit de AVG en daarop gebaseerde Nederlandse wetgeving is neergelegd bij de AP. De Autoriteit Consument en Markt houdt toezicht op naleving van andere regelgeving die - direct of indirect - de bescherming van de privacy dient. Te denken valt aan het telecommunicatierecht en het consumentenrecht.

De Politie en het OM hebben een handhavende rol bij overtreding van strafrechtelijke wetsbepalingen op het terrein van privacybescherming. Denk aan het heimelijk filmen of opnemen van gesprekken, huisvredebreuk, computervredebreuk en stalking.

5. Agenda horizontale privacy

Burgers moeten zich vrij en veilig kunnen voelen in een digitaliserende wereld, waarin technologische ontwikkelingen niet alleen kansen bieden, maar ook risico's meebrengen voor hun privacy en individuele vrijheid en veiligheid.

Het kabinet zet daarom in op:

- vergroting van het privacybewustzijn,
- vergroting van het handelingsperspectief en
- versterking van de normering.

5.1 Vergroting privacybewustzijn

Privacybescherming begint ermee dat iemand zich bewust is van de risico's die zijn handelen voor de privacy van een ander of die van hemzelf heeft. Vergroting van dat bewustzijn kan er in belangrijke mate aan bijdragen dat iemand beter gaat nadenken alvorens hij in de vorm van beeld of tekst informatie over zichzelf of over een ander vastlegt en met anderen deelt. Het kan om informatie gaan

waarvan hijzelf of die ander liever niet heeft dat deze nog verder verspreid wordt. Tegen deze achtergrond neemt het kabinet een aantal maatregelen om het privacybewustzijn te vergroten.

Voorlichting

Vergroting van het privacybewustzijn kan worden bereikt door goede voorlichting. Het kabinet zal daarom in het voorjaar van 2020 een grote publiekscampagne starten die burgers meer bewust moet maken van de privacyrisico's bij het gebruik van bijvoorbeeld digitale applicaties. Het is belangrijk dat mensen meer bewust worden van de gevolgen die het delen van persoonlijke data met zich meebrengt. Gedacht wordt aan een campagne die in ieder geval online wordt uitgevoerd, via social media en mogelijk ook op radio en televisie.

In aanvulling op de voorlichting die de AP al over de AVG geeft, is zij vanaf 25 mei van dit jaar daarover voorlichting gaan geven die specifiek voor het MKB bestemd is. Daarnaast geeft de AVG helpdesk Zorg, Welzijn en Sport van het ministerie van VWS voorlichting over de AVG aan organisaties op deze terreinen.

Verder heeft het kabinet het project 'de Maatschappelijke Dialoog' ontwikkeld. Onder regie van BZK gaan burgers, ondernemers, medeoverheden, toezichthouders en wetenschappers met elkaar in gesprek over grondrechten en publieke waarden bij de ontwikkeling van nieuwe technologie. Privacybescherming is hiervan een belangrijk onderdeel.

Er wordt een webportaal voor burgers en bedrijven ontwikkeld waarop ook voorlichting zal worden gegeven (zie hierna bij 'Privacywijzer voor burgers en bedrijven).

Herziening onderwijscurriculum

Kinderen raken op steeds jongere leeftijd in aanraking met social media. Het is daarom wenselijk kinderen al op jonge leeftijd te leren verantwoord met social media om te gaan. Met het oog daarop is van belang dat het curriculum voor het primair en voortgezet onderwijs op dit moment integraal wordt herzien.[16] Een veilige en verantwoorde omgang met sociale media zal daarbij een belangrijk onderwerp zijn binnen het leergebied 'Digitale geletterdheid'. Daarbinnen wordt ook aandacht besteed aan het bewust en kritisch omgaan met de mogelijkheden van digitaal communiceren en publiceren. De resultaten van de ontwikkelteams die het nieuwe onderwijscurriculum voorbereiden, worden kort na de zomer van 2019 opgeleverd.

5.2. Vergroting handelingsperspectief

Burgers hebben instrumenten nodig om hun privacy te beschermen en zich tegen privacyschendingen te kunnen verweren. Daarnaast hebben bedrijven instrumenten nodig om de privacyregelgeving te kunnen naleven. Het kabinet neemt daartoe de volgende maatregelen.

Privacywijzer voor burgers en bedrijven

Het Platform voor de Informatiesamenleving ECP ontwikkelt op verzoek van het ministerie van JenV een webportaal (de Privacywijzer) met praktische

[16] https://curriculum.nu/ontwikkelproces.

handreikingen die mensen helpen bij het uitoefenen van hun rechten die zij op basis van de AVG hebben. Het gaat dan bijvoorbeeld om inzageverzoeken of zogeheten vergetelheidsverzoeken om de persoonsgegevens die in het bezit zijn van bedrijven te wissen.

Bedrijven kunnen op het hetzelfde portaal hulpmiddelen vinden om bijvoorbeeld een privacyverklaring op te stellen. Ook kunnen zij daarop voorbeelden laten zien van hoe zij toestemming vragen om persoonsgegevens te mogen gebruiken. Op die manier kan op deze punten een zekere standaardisering ontstaan, zoals in de initiatiefnota 'Onderlinge privacy' en een motie Van Nispen is bepleit, terwijl ook rekening kan worden gehouden met de verschillen tussen bedrijven in omvang, functies en businessmodel. [17]

De Privacywijzer voor burgers en bedrijven is medio 2019 gereed.

Laagdrempelige voorziening om privacyschendend beeldmateriaal van internet te verwijderen

Het kabinet wil een gebruiksvriendelijke voorziening voor burgers om beeldmateriaal op internet – dat tot hem of haar te herleiden is maar zonder toestemming is geplaatst – op een snelle wijze te laten verwijderen. Voorbeelden waarin zo'n voorziening uitkomst kan bieden, zijn online pesten, stalking, bedreiging, wraakporno, het posten van (seksueel getinte) privé opnames en *slut shaming* (anderen voor slet uitmaken).

Ik laat met mijn ambtgenoot van Justitie en Veiligheid een haalbaarheidsstudie uitvoeren naar een dergelijke voorziening. In die studie wordt onderzocht hoe een dergelijke voorziening er precies uit kan zien, of deze taak kan worden neergelegd bij de rechterlijke macht of bij een reeds bestaande toezichthouder en hoe de kosten die ermee zijn gemoeid zoveel mogelijk kunnen worden beperkt. Deze studie wordt nog in deze kabinetsperiode afgerond en voorzien van een reactie. Dit zal, afhankelijk van de uitkomst van de haalbaarheidsstudie, tot de invoering van zo'n voorziening leiden.

Daarmee komt het kabinet tegemoet aan het voorstel uit de initiatiefnota 'Onderlinge privacy' om slachtoffers van evidente privacyschendingen een spoedprocedure te bieden om de schadelijke content van internet te verwijderen, naar analogie van het zogeheten ex parte-verbod uit het intellectuele eigendomsrecht.[18] Met een dergelijke voorziening wordt ook uitvoering gegeven aan de motie Van Nispen waarin de regering wordt verzocht een voorstel uit te werken voor een snelle, laagdrempelige procedure om privacyschendingen op internet snel te beëindigen en slachtoffers beter te ondersteunen.[19]

Verbetering collectieve procedures

Bij de verwerking van persoonsgegevens in een big-data-toepassing kan er sprake zijn van een schending van de privacy van een grote groep mensen. Om een dergelijk collectief belang beter te kunnen behartigen, vindt het kabinet het wenselijk de mogelijkheden van het voeren van een collectieve actie te verbeteren.

[17] Kamerstukken II 2017/18, 34926, nr. 2, p. 5, en 32761, nr. 121.
[18] Kamerstukken II 2017/18, 34926, nr. 2, p. 4-5.
[19] Kamerstukken II 2017/18, 34926, nr. 6.

Op dit moment onderzoekt de Tilburg University op verzoek van het ministerie van JenV hoe deze mogelijkheden kunnen worden uitgebreid door bijvoorbeeld de wetgeving op dat punt aan te passen. Met dit onderzoek wordt ook uitvoering gegeven aan de motie Buitenweg waarin de regering met het oog op de effecten van dataverwerkingsprojecten op de samenleving is verzocht om mogelijkheden voor het verruimen van collectieve procedures bij de rechter te onderzoeken en de Kamer hierover te informeren.[20] Het kabinet informeert de Kamer voor het eind van het jaar over de conclusies die aan het onderzoeksrapport zullen worden verbonden, en over eventuele wetgeving die daarop zal volgen. Daarbij wordt ook de recent aangenomen Wet afwikkeling massaschade in collectieve actie (Stb. 2019, 130) betrokken. In dit verband wordt verder gekeken naar een Duits voorbeeld ter versterking van de handhavingsmogelijkheden voor consumentenorganisaties en kamers van koophandel om tegen schendingen van voorschriften uit het gegevensbeschermingsrecht te kunnen optreden.[21]

5.3 Versterking normering

Tot slot moeten de normen waarmee privacy wordt beschermd, een adequaat niveau van bescherming bieden. Hierbij moet in voldoende mate rekening worden gehouden met de risico's die sommige technologische ontwikkelingen meebrengen. Met het oog daarop wil het kabinet de volgende maatregelen treffen.

<u>Strafbaarstelling wraakporno</u>

Mede ter uitvoering van het regeerakkoord[22] wil het kabinet misbruik van seksueel beeldmateriaal (wraakporno) zelfstandig strafbaar stellen en heeft het hiervoor een wetsvoorstel bij de Tweede Kamer ingediend.[23] De reden daarvan is dat wraakporno een ernstige aantasting van de privacy kan opleveren. Strafbaarstelling draagt bij aan een eenduidige strafrechtelijke aanpak en zorgt voor erkenning van leed dat slachtoffers wordt aangedaan. Van specifieke strafbaarstelling gaat tevens het signaal uit aan (potentiële) daders dat dit type gedrag niet acceptabel is.

<u>Aanpak filmen van verkeersslachtoffers en andere hulpbehoevenden</u>

Het fotograferen of filmen van verkeersslachtoffers en andere personen in hulpbehoevende toestand grijpt diep in op de privacy van betrokkenen en hun naasten en is dan ook verwerpelijk. Ik zie het initiatiefwetsvoorstel tegemoet dat het lid Van Toorenburg heeft aangekondigd om publicatie van beeldmateriaal van (verkeers)slachtoffers strafbaar te stellen.

Vooruitlopend op het initiatiefwetsvoorstel zal een publiekscampagne van start gaan om mensen op hun verantwoordelijkheid aan te spreken en de consequenties van hun handelen te laten inzien. Zo wordt publiekelijk de norm nog eens extra onderstreept. Voor het opzetten van de campagne zal gebruik worden gemaakt van de resultaten van enquêtes die het Rode Kruis en de politie

[20] Kamerstukken II 2017/18, 32 761, nr. 119.
[21] Zie de 'Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts' (Bundesgesetzblatt 2016, Teil I, nr. 8). Het gaat hierbij om schendingen bij verwerking van persoonsgegevens van consumenten door een ondernemer voor bijvoorbeeld reclame, marketing of profilering.
[22] Vertrouwen in de toekomst. Regeerakkoord 2017–2021, p. 6.
[23] Zie Kamerstukken II 2018/19, 35080, nrs. 1-3, en ook onderdeel f van de bijlage.

hebben uitgezet onder hulpverleners over hun ervaringen met het filmen van (verkeers)slachtoffers.[24]

Aanscherping AVG in relatie tot de datamacht grote techbedrijven en profilering

De AVG legt aan grote techbedrijven die persoonsgegevens verwerken, verplichtingen op om die gegevens goed te beschermen. Dergelijke bedrijven zijn in staat om, ook als zij in overeenstemming met de AVG handelen, zeer veel persoonsgegevens over individuen te verzamelen. Het kabinet onderzoekt of de wettelijke eisen in de AVG ten aanzien van deze bedrijven kunnen worden aangescherpt om de hoeveelheden gegevens die zij over personen verwerken te beteugelen. Het wil daarnaast wettelijke voorschriften die specifieker zijn dan die in de AVG om risico's van profilering tegen te gaan. Daarbij moet gedacht worden aan risico's dat personen op basis van een profiel van (het aanbieden van) producten en diensten worden uitgesloten of daarvoor hogere prijzen moeten betalen, zonder dat daarvoor een terechte grond bestaat. Het kabinet zal dit onderdeel laten zijn van de evaluatie van de AVG, die in mei 2020 moet zijn afgerond.

Mededingingsbeleid in relatie tot online platforms

Naast privacyregelgeving kan ook mededingingsregelgeving soelaas bieden als het gaat om privacy-inbreuken die het gevolg zijn van uit de hand gelopen machtsposities van bepaalde bedrijven. In Europees verband bepleit de staatssecretaris van EZK op korte termijn om de Europese richtsnoeren die de mededingingsregels uitleggen, beter toepasbaar te maken voor online platforms.[25] Daarbij kan worden overwogen om in die richtsnoeren vast te leggen op welke manier misbruik van een machtspositie, door bijvoorbeeld een groot techbedrijf mede gebaseerd kan worden op privacy of data. Hierbij zal onder andere worden gekeken naar een recente uitspraak van het Bundeskartellamt dat oordeelde dat Facebook misbruik maakt van zijn machtspositie door de data die het bedrijf verzamelt.

Inventarisatie risico's nieuwe technologische ontwikkelingen

Het kabinet acht het wenselijk om in de toekomst bij nieuwe technologische ontwikkelingen in een veel vroeger stadium dan nu het geval is systematisch na te denken over de risico's die deze technieken voor de privacy hebben. Zo kunnen tijdig maatregelen worden ontwikkeld om risico's te mitigeren. Om te beginnen zal onderzoek worden gedaan naar de risico's van gezichtsherkenningstechnologie en commercieel DNA-gebruik.

Vanwege de snelle opmars van het gebruik van gezichtsherkenningstechnologie moet er beter zicht komen op de risico's die deze technologie voor de privacy heeft, en welke maatregelen getroffen kunnen worden om deze risico's te beperken. Aan de hand van gezichtsherkenningstechnologie is het ook voor particulieren in de toekomst mogelijk om iemand razendsnel te identificeren. Ik laat om die reden door de Tilburg University een verkenning uitvoeren. Dit onderzoek is naar verwachting eind dit jaar gereed.

Bij gebruik van DNA-materiaal doet zich de bijzondere omstandigheid voor dat het om persoonsgegevens gaat die op meer dan één persoon betrekking hebben,

[24] Handelingen II 2018/19, 27, item 10, p. 8.
[25] Kamerstukken II 2018/19, 27879, nr. 71, p. 8.

namelijk ook op de directe verwanten van degene die toestemming voor het gebruik daarvan heeft gegeven. Dat betekent dat DNA-identificatie door één persoon ook gegevens bloot kan leggen over personen die daar niet om hebben gevraagd en dit ook niet wensen. In het licht van de bijzondere risico's die dit voor de privacy van betrokkenen meebrengt, acht ik het wenselijk deze risico's bij commercieel gebruik van DNA te beperken en te onderzoeken hoe dat kan. Ik verwacht u tegen het eind van het jaar daarover te kunnen informeren.

Beteugeling spyware

Als gevolg van technologische ontwikkelingen zijn producten waarmee gemakkelijk kan worden gespioneerd goedkoper en makkelijker beschikbaar. Nu vormen heimelijk filmen, computervredebreuk en heimelijk afluisteren een zeer ernstige schending van de privacy en zijn zij daarom strafbaar.[26] De vraag doet zich echter voor of er in aanvulling op de nu bestaande strafrechtelijke aanpak ook andere manieren zijn om spyware te reguleren en de privacyrisico's te verminderen. Hetzelfde geldt met betrekking tot het gebruik van drones. Daarom laat ik door de Tilburg University onderzoeken wat de mogelijkheden daartoe zijn. In dat onderzoek wordt onder meer aandacht besteed aan vergunningenstelsels in andere landen voor de verkoop van spionageproducten.[27] Het onderzoek is naar verwachting begin 2020 gereed. Afhankelijk van de uitkomst daarvan kom ik daarna met maatregelen.

Daarnaast wil het kabinet voor de aanpak van privacyschendingen door drones de mogelijkheden bezien die de komende Europese verordening over drones biedt om een aspect als privacy te laten meewegen voor het instellen van zones waarbinnen drones wel of niet mogen worden gebruikt.[28]

Privacywaarborgen smart cities

Bij de verdere ontwikkeling van *smart cities* moeten voldoende waarborgen worden getroffen om de privacy te beschermen. Met het oog daarop is van belang dat onder regie van BZK en in samenwerking met de VNG bij een aantal grote gemeenten pilots worden uitgevoerd om tot normen voor de inrichting van smart cities te komen.[29] Daarnaast wordt gewerkt aan een 'Code goed digitaal openbaar bestuur', waarin beginselen van deugdelijk digitaal overheidsbestuur zijn vastgelegd die organisaties in het openbaar bestuur in gedragsregels moeten uitwerken. Deze code, die in de tweede helft van 2019 gereed is, zal mede van belang zijn voor bescherming van de privacy bij de verdere ontwikkeling van smart cities en de relatie met burgers en bedrijven binnen dat concept.

Minimumveiligheidseisen IoT-apparaten

De koppeling van apparaten via het internet (IoT) biedt ongekende mogelijkheden. Maar als de beveiliging niet goed is geregeld, kan het ook ernstige inbreuken op de privacy veroorzaken. Als onderdeel van de 'Roadmap Digitaal Veilige Hard- en Software' wordt op initiatief van Nederland in EU-verband onderzocht welke minimumveiligheidseisen gesteld kunnen worden aan IoT-apparaten, zoals smart watches en interactief speelgoed. Door middel van de Radio Equipment Directive (RED) kunnen onveilige apparaten, die bijvoorbeeld

[26] Zie de artikelen 139a-139f en 441b Wetboek van Strafrecht.
[27] Zie ook de onderdelen h en j van de bijlage.
[28] Zie Kamerstukken II 2018/19, 30806, nr. 48.
[29] Data Agenda Overheid, bijlage bij Kamerstukken II 2018/19, 26643, nr. 597.

voor ongewilde kennisneming van spraakcommando's zorgen, van de markt worden geweerd.[30]

Versterking Autoriteit persoonsgegevens

Normering kan niet zonder goed toezicht en handhaving, zoals het opleggen van boetes. In het kader van die toezichts- en handhavingstaken is met de komst van de AVG het budget van de Autoriteit persoonsgegevens (AP) bijna verdubbeld: aan het budget is vanaf 2018 structureel € 5 miljoen toegevoegd en vanaf 2019 nog eens structureel € 2 miljoen. In de Voorjaarsnota is een verdere structurele verhoging van het budget met € 3,4 miljoen opgenomen. Het voor de AP beschikbare budget komt daarmee in 2019 op € 18,5 miljoen. Dit komt het toezicht op de bescherming van persoonsgegevens ten goede.

6. Slot

De 'Agenda horizontale privacy' bevat maatregelen en acties die naar het oordeel van het kabinet nu het meest urgent zijn. In de nabije toekomst zullen nieuwe onderwerpen opkomen. Die worden dan aan deze agenda toegevoegd. De agenda groeit dus met de actualiteit.

In dat verband blijven we in nauw contact met vertegenwoordigers van de wetenschap, het bedrijfsleven en organisaties die het privacybelang behartigen, en volgen we evenzeer nauwgezet de toekomstige technologische ontwikkelingen.

Ik informeer uw Kamer voor de zomer van 2020 over de uitvoering van deze agenda of zoveel eerder als dat met betrekking tot een specifiek onderwerp is aangekondigd.

De Minister voor Rechtsbescherming,

Sander Dekker

[30] Zie ook onderdeel e van de bijlage.

Bijlage bij de brief over 'Bescherming horizontale privacy'

Deze bijlage heeft betrekking op de voorstellen uit de initiatiefnota 'Onderlinge privacy' van het lid van uw Kamer Koopmans[31] en de reactie van het kabinet daarop. De bijlage volgt daarbij de lettering van deze voorstellen in die initiatiefnota.

a. Laagdrempelige mogelijkheid om beeldmateriaal te verwijderen dat de privacy schendt

In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld om slachtoffers van evidente privacyschendingen een spoedprocedure bij de civiele rechter te bieden om de schadelijke content van internet te verwijderen, naar analogie van het zogeheten ex parte-verbod uit het intellectuele eigendomsrecht.

Om de mogelijkheid van een ex parte procedure te toetsen op haalbaarheid laat het kabinet onderzoeken in hoeverre de voorgenomen procedure overlapt met bestaande procedures (bij de civiele rechter en bij de AP), en hoe een dergelijke ex parte procedure er precies uit zou kunnen zien. Daarnaast is, met het oog op de praktische uitvoerbaarheid van een ex parte procedure over online content, van belang een beeld te krijgen van de omvang van de huidige problematiek. Deze studie wordt nog in deze kabinetsperiode afgerond en voorzien van een reactie. Dit zal, afhankelijk van de uitkomst van de haalbaarheidsstudie, tot de invoering van zo'n voorziening leiden.

b. Faciliteren van online aangifte bij onderlinge privacy-schendingen

In de initiatiefnota 'Onderlinge privacy' wordt bepleit om slachtoffers van onderlinge privacy-schendingen te faciliteren met de mogelijkheid om daarvan online aangifte te doen.

Op dit moment is het nog niet mogelijk om voor ieder strafbaar feit (met opsporingsindicatie) online aangifte te doen. De politie streeft er wel naar de mogelijkheden van online aangifte uit te breiden.

c. Vergroting kennis over onderlinge privacy bij politie, OM en rechterlijke macht

In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld de kennis over onderlinge privacy bij politie, OM en rechterlijke macht te vergroten.

In veel gevallen zijn politie, OM en rechter al voldoende toegerust om binnen het strafproces de juiste hulp te bieden. Het gaat hier onder meer om zedenzaken die ook al voor het digitale tijdperk regelmatig voorkwamen, en waar politie en OM ervaring mee hebben. Zo beschikken zij over specialisten op dit terrein en zijn er expertisecentra die kennis hebben, ontwikkelen en verspreiden onder de betrokken organisaties. Deze organisaties hebben ook specifieke aandacht voor dit type gevallen. Door de toenemende digitalisering komt dit soort zaken vaker voor en, gelet op de impact op de slachtoffers, betekent dit ook een groeiende aandacht van politie en OM.

Toch zijn er enkele sleutelmomenten waarbij extra alertheid is geboden om de juiste hulp te bieden aan het slachtoffer. Als er sprake is van een strafbaar feit

[31] Kamerstukken II 2017/18, 34926, nr. 2.

waarvan aangifte wordt gedaan, wordt het slachtoffer daarin begeleid. Daarbij moet met de menselijke bril gekeken worden naar wat het slachtoffer nodig heeft. In verband daarmee wordt sinds 1 juni 2018 de zogenoemde Individuele Beoordeling fasegewijs ingevoerd. Die zorgt voor een betere bescherming van slachtoffers door bij ieder slachtoffer, vanaf het moment van melden bij de politie, te kijken naar kwetsbaarheid voor herhaald slachtofferschap.

Een ander sleutelmoment betreft het moment van overdracht van een zaak door de politie aan het OM. Zij hebben afspraken gemaakt over de aanduiding van het soort zaak, zodat het in de hele keten duidelijk zichtbaar is wat voor type zaak het is en welke aandacht en prioriteit er bij hoort. Politie en OM voeren overleg om te waarborgen dat deze afspraken ook passen bij alle vormen van (strafbare) schendingen van de privacy.

d. Versterken van het recht op vergetelheid

Artikel 17 AVG geeft het recht op vergetelheid, d.w.z. het recht van betrokkenen om hem betreffende persoonsgegevens zonder onredelijke vertraging door de verwerkingsverantwoordelijke te laten wissen. In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld de uitoefening van dit recht te versterken door het doen van aangifte mee te laten wegen in het urgent honoreren van een verzoek.

Bij het ontwikkelen van de Privacywijzer burger en bedrijven[32] wordt bezien in hoeverre aan dit voorstel uitvoering kan worden gegeven.

e. Bescherming tegen privacy-risico's van internet of things

Steeds meer apparaten worden met het internet verbonden. Als deze apparaten niet goed zijn beveiligd, kunnen via deze 'internet of things apparaten' (IoT-apparaten) ongemerkt persoonsgegevens worden verzameld en kunnen met het internet verbonden apparaten worden misbruikt om bijvoorbeeld DDoS-aanvallen uit te voeren.

Tegen deze achtergrond wordt in de initiatiefnota 'Onderlinge privacy' voorgesteld om bij de uitwerking van de voorgenomen Europese standaarden voor IoT-apparaten samen met het bedrijfsleven bijzondere aandacht te geven aan de privacy-risico's van producten die een aanzienlijk privacy-risico kennen. Daarbij wordt onder meer gedacht aan spraakconsoles in huis en met het internet verbonden auto's.

Om de veiligheid te bevorderen van hard- en software, waaronder IoT-apparaten, is de Roadmap Digitaal Veilige Hard- en Software opgesteld die op 23 april 2018 naar de Tweede Kamer is gezonden.[33] De roadmap bevat een samenhangende set van maatregelen om onveiligheid in hard- en software te voorkomen, kwetsbaarheden te detecteren en om de gevolgen daarvan te beperken. Het bevorderen van de digitale veiligheid draagt bij aan de bescherming van persoonsgegevens. Zo wordt bijvoorbeeld op initiatief van Nederland in EU-verband onderzocht welke minimumveiligheidseisen door middel van de Radio Equipment Directive (RED) gesteld kunnen worden aan IoT-apparaten zoals *smart watches* en interactief speelgoed, zodat onveilige apparaten van de markt

[32] Zie § 5.2 van de brief.

[33] Kamerstukken II 2017/18, 26 643, nr. 535, met bijlage.

geweerd kunnen worden.[34] Onveilige apparaten kunnen bijvoorbeeld voor ongewilde kennisneming van spraakcommando's zorgen.

Nederland heeft daarnaast bij de voorbereiding van de Cybersecurity Act gepleit voor verplichte certificering van ICT-producten en –diensten. Vooralsnog zijn er geen lidstaten die Nederland daarin steunen, maar Nederland zal hiervoor blijven pleiten conform de motie van het lid van uw kamer Paternotte.[35]

f. Zelfstandige strafbaarstelling van misbruik van seksueel beeldmateriaal

In de initiatiefnota 'Onderlinge privacy' wordt een brede strafbaarstelling van wraakporno bepleit. Daartoe heeft het kabinet inmiddels een wetsvoorstel ingediend.[36]

g. Slachtofferhulp voor online privacy-schendingen

In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld de hulp aan slachtoffers van evidente ernstige privacy-schendingen te verbeteren.

De hulplijn Help Wanted van het Expertisecentrum Online Kindermisbruik (EOKM) biedt informatie en advies aan kinderen en jongeren tot 26 jaar, hun opvoeders, hulpverleners en docenten die te maken hebben (gehad) met online seksueel misbruik (zoals wraakporno). Verder biedt Slachtofferhulp Nederland in meer algemene zin hulp aan slachtoffers van strafbare feiten. De hulp die aldus aan slachtoffers van strafbare privacy-schendingen kan worden geboden, acht het kabinet voldoende.

h. Beperking verkoop spionageproducten

Door technologische vernieuwing kunnen steeds meer producten worden ontwikkeld waarmee gemakkelijk kan worden gespioneerd. Denk aan geminiaturiseerde camera's en locatie-trackers die ongemerkt worden aangebracht, en spionagesoftware. Gebruik van dergelijke producten kan een forse inbreuk op de privacy betekenen. In de initiatiefnota 'onderlinge privacy' wordt daarom bepleit de mogelijkheid te onderzoeken om een vergunningenstelsel te introduceren voor de verkoop van specifiek voor spionage bedoelde producten, zoals spy-camera's en spionagesoftware.

De huidige wetgeving bevat al verschillende mogelijkheden om tegen de verkoop van spionagesoftware op te treden. Als bijvoorbeeld iemand spionagesoftware verkoopt met het oogmerk dat daarmee computervredebreuk wordt gepleegd of telecommunicatie wordt afgetapt, dan is die persoon op grond van artikel 139d, tweede lid, onder a, van het Wetboek van Strafrecht (Sr) strafbaar. Als spy-camera's heimelijk worden gebruikt om iemand in een woning of op een andere niet voor het publiek toegankelijke plaats te filmen, is dat op grond van artikel 139f Sr in beginsel strafbaar. En gebeurt dit heimelijk filmen op een voor het publiek toegankelijke plaats, dan kan sprake zijn van strafbaar handelen op grond

[34] In het kader van de RED kan de Europese Commissie eisen stellen aan daarbij nader te bepalen categorieën telecommunicatieapparatuur ter bescherming van de veiligheid van gebruikers (security by design). Daarbij geldt een systeem van verplichte (zelf)certificering. Nederland bepleit in dit verband een brede toepassing van deze eisen op IoT-apparaten.
[35] Kamerstukken II 2017/18, 21501-33, nr. 717, p. 2; Kamerstukken II 2017/18, 21501-30, nr. 422. Kamerstukken II 2018/19, 27 879, nr. 64, p. 5.
[36] Zie ook § 5.3 van de brief.

van artikel 441b Sr. In het licht van artikel 139d Sr is ook het wederrechtelijk gebruik van een locatie-tracker strafbaar. Relevant is voorts artikel 441a Sr waarin een verbod is opgenomen tot het maken van reclame e.d. voor afluister- en opneemapparatuur of onderdelen daarvan.

Naast de mogelijkheden om strafrechtelijk tegen voor spionage bedoelde producten op te treden, kan eventueel een vergunningenstelsel toegevoegde waarde hebben. Met het oog daarop laat ik de Tilburg University onderzoeken of er landen zijn waar een vergunningenstelsel voor de verkoop van specifiek voor spionage bedoelde producten, zoals spy-camera's en spionagesoftware, bestaat en, zo ja, hoe deze stelsels zijn ingericht. Daarbij wordt ook onderzocht in hoeverre het in het licht van de regels van de EU met betrekking tot de vrije markt mogelijk is zo'n stelsel ook in Nederland te introduceren. Dit onderzoek is naar verwachting begin 2020 gereed. Afhankelijk van de uitkomst daarvan kom ik daarna met maatregelen.

i. Bescherming tegen privacy-risico's van gezichtsherkenningstechnologie

In de initiatiefnota 'Onderlinge privacy' wordt gepleit voor een onderzoek naar regulering van het privé-gebruik van gezichtsherkenningstechnologie.

Op dit moment laat ik de Tilburg University een verkennend onderzoek uitvoeren naar de risico's van gezichtsherkenning en naar bestaande juridische middelen in bijvoorbeeld het auteursrecht en het gegevensbeschermingsrecht om deze risico's te beperken. Het onderzoek strekt zich ook uit naar 'best practices', interne procedures of anderszins praktische waarborgen die bedrijven hanteren bij het gebruik van gezichtsherkenning om deze risico's zoveel mogelijk te beperken en naar aanvullende middelen om deze risico's ook in de nabije toekomst het hoofd te kunnen bieden. Daarbij wordt ook een blik geworpen op goede voorbeelden in andere landen. Dit onderzoek is naar verwachting eind dit jaar gereed. Afhankelijk van de uitkomst daarvan kom ik daarna met maatregelen.

j. Bescherming tegen privacy-risico's van het gebruik van drones

In de initiatiefnota 'Onderlinge privacy' wordt gevraagd om een onderzoek naar praktische waarborgen tegen de privacy-risico's van het gebruik van hobbydrones. Deze vraag wordt meegenomen in een onderzoek dat ik laat uitvoeren naar de vraag hoe het gebruik van spionageproducten en drones door burgers beter kan worden gereguleerd teneinde de privacy van de burger beter te kunnen beschermen (zie ook onderdeel h). Afhankelijk van de uitkomst daarvan kom ik daarna met maatregelen.

k. Standaardprotocollen voor vergetelheidsverzoeken

In voornoemde initiatiefnota wordt ook bepleit samen met het bedrijfsleven standaardprotocollen voor vergetelheidsverzoeken te ontwikkelen. Dit moet gebeuren zonder aantasting van de vrije meningsuiting, de persvrijheid en zonder onbedoeld fraudeurs te beschermen. Met het oog hierop zullen op de Privacywijzer burger en bedrijven[37] voorbeelden worden getoond van hoe bedrijven vergetelheidsverzoeken afhandelen. Zo kan er enige uniformering hierin ontstaan, terwijl ook rekening kan worden gehouden met de verschillen tussen bedrijven in omvang, functies en businessmodel.

[37] Zie § 5.2 van de brief.

l. Bescherming tegen heimelijk opnemen van privé-gesprekken

In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld een toestemmingsvereiste in te voeren voor het stiekem opnemen van privégesprekken, behoudens een evident publiek belang, zoals in bepaalde gevallen onderzoeksjournalistiek. Het kabinet is van mening dat de bescherming tegen het stiekem opnemen van privégesprekken al afdoende is geregeld.

Zo is het afluisteren of opnemen van vertrouwelijke communicatie in verschillende bepalingen in het Wetboek van Strafrecht strafbaar gesteld. Daarbij wordt onderscheid gemaakt tussen het met een technisch hulpmiddel afluisteren of opnemen van een gesprek dat wordt gevoerd in een woning, besloten lokaal of erf (zie artikel 139a Sr) en het aftappen of opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of een geautomatiseerd werk (artikel 139c Sr). Bij dat laatste kan worden gedacht aan telefoongesprekken. In alle gevallen geldt de voorwaarde dat de dader zelf niet deelneemt aan het gesprek en ook niet handelt in opdracht van iemand die wel deelneemt aan het gesprek, dan wel – in geval van bijvoorbeeld telefoongesprekken – dat deze niet voor de dader bestemd zijn. De strafbepalingen betreffen dus communicatie tussen andere personen. De wetgever meende dat het opnemen van gesprekken door een van beide gespreksdeelnemers weliswaar onethisch kan zijn, of onrechtmatig kan zijn jegens de andere gespreksdeelnemer(s), maar dat het minder passend was dit strafbaar te stellen.[38] Het kabinet ziet geen aanleiding om dit thans anders te beoordelen, reeds omdat hierdoor bijvoorbeeld het opnemen van gesprekken door journalisten of slachtoffers van stalking in beginsel strafbaar zou worden (of door de introductie van een toestemmingsvereiste tandeloos). Een evident publiek belang, zoals de vrijheid van nieuwsgaring, kan onder omstandigheden nu al de onrechtmatigheid van het stiekem opnemen opheffen. Met een en ander is de bescherming tegen het stiekem opnemen van privégesprekken al afdoende geregeld.

m. Vergroting maatschappelijk bewustzijn

Bescherming van je privacy begint met je bewust te zijn van de risico's die je in het dagelijks leven op dit punt loopt, en van de mogelijkheden om je daartegen te beschermen. Voor de ontwikkeling van dit bewustzijn zijn transparantie, voorlichting en onderwijs van groot belang. Op dit vlak is al veel in gang gezet, maar zijn ook nieuwe maatregelen in voorbereiding, die in § 5.1 van de brief worden beschreven. Met deze maatregelen wordt naar het oordeel van het kabinet voldoende tegemoet gekomen aan het voorstel uit de initiatiefnota 'Onderlinge privacy' om het maatschappelijk bewustzijn over de eigen verantwoordelijkheid bij privacybescherming te vergroten.

n. Europese en internationale samenwerking ter versterking van de onderlinge privacy

In de initiatiefnota 'Onderlinge privacy' wordt een pleidooi gehouden voor Europese en internationale samenwerking ter versterking van de onderlinge privacy.

De grondrechten privacy en bescherming van persoonsgegevens zijn verankerd in Europese en internationale verdragen. De bescherming van persoonsgegevens is

[38] Kamerstukken II 1967/68, 9419, nr. 3, p. 5.

versterkt met de komst van de AVG. De versterking daarvan heeft mede betrekking op de relatie tussen burgers onderling.

Internationaal wordt zowel in multilaterale als in multistakeholder gremia gesproken over de bescherming van privacy in het digitale tijdperk. Deze discussies spitsen zich met name toe op de relatie tussen burgers enerzijds en bedrijven dan wel overheden anderzijds. Nederland neemt een vooraanstaande positie in ten aanzien van het pleiten voor een vrij en open internet waarbij sprake is van gelijke waarborging van grondrechten online en offline. Het kabinet werkt op internationaal niveau samen met andere landen om deze boodschap uit te dragen en concreet bij te dragen aan het verankeren en naleven van grondrechten in het digitale tijdperk.

Een belangrijk normstellend document is de VN-resolutie over Privacy in a Digital Age. Het mensenrechtenbureau van de VN in Genève faciliteert een internationale discussie over dit thema, door een workshop te organiseren en een rapport op te stellen. Nederland draagt bij aan deze discussie waar bijvoorbeeld de vraag op tafel ligt of een nieuw wetgevend instrument, zoals een verdrag, nodig is om privacy in het digitale tijdperk beter te beschermen.

o. Onderlinge privacybescherming in het buitenland

In de initiatiefnota 'Onderlinge privacy' wordt voorgesteld onderzoek te doen naar de onderlinge privacybescherming in het buitenland, waaronder het Duitse grondrecht van 'Informationelle Selbstbestimmung'. Het WODC is gevraagd hiernaar onderzoek uit te voeren. Dit onderzoek is naar verwachting begin 2020 gereed.

p. Dialoog met mensen, bedrijven en organisaties uit de praktijk

Voor het creëren van voldoende draagvlak voor het kabinetsbeleid met betrekking tot de bescherming van de horizontale privacy is van belang dat bij de ontwikkeling daarvan ook organisaties en bedrijven worden betrokken die hiervoor relevante inbreng kunnen leveren. Het kabinet onderschrijft dan ook het pleidooi in de initiatiefnota 'Onderlinge privacy' om mensen, bedrijven en organisaties uit de praktijk te betrekken bij het ontwikkelen van ideeën, het 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. Vertegenwoordigers van mijn ministerie hebben dan ook regelmatig contact met vertegenwoordigers van het bedrijfsleven en organisaties die het privacybelang behartigen, om met elkaar daarover van gedachten te wisselen. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties richt zich op de brede dialoog over publieke waarden en mensenrechten en de waarborging hiervan in de informatiesamenleving.

Op 16 mei 2018 heb ik een gesprek gevoerd met vertegenwoordigers van Google, Facebook en Microsoft, VNO/NCW en brancheverenigingen Nederland ICT over onder meer de vraag wat het bedrijfsleven kan bijdragen aan een betere bescherming van de horizontale privacy. Dit heeft mede geleid tot het plan om een Privacywijzer voor burgers en bedrijven te ontwikkelen. Vervolgens heb ik op 11 maart jl. met partijen gesproken over de ethische aspecten van toepassing van Big Data en artificiële intelligentie. Het is evident dat privacybescherming daarvan een belangrijk onderdeel uitmaakt. In de toekomst zet ik deze dialoog voort.