Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

34 926 Initiatiefnota van het lid Koopmans: Onderlinge privacy

Nr. 11 **BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 februari 2021

Op 7 juni 2019 zond ik u de kabinetsvisie op de bescherming van de horizontale privacy. In die visie 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.[1]

Om dit doel te bereiken heeft het kabinet een Agenda horizontale privacy opgesteld waarin wordt ingezet op:
- vergroting van het privacybewustzijn,
- vergroting van het handelingsperspectief en
- versterking van de normering.[2]

Aan het slot van de kabinetsvisie heb ik u toegezegd uw Kamer voor de zomer van 2020 te informeren over de uitvoering van de maatregelen die in deze agenda zijn genoemd. Door COVID-19 heeft de uitvoering van deze toezegging enige vertraging opgelopen. Met deze brief doe ik deze toezegging mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties alsnog gestand.

1. Vergroting privacybewustzijn

Voorlichting

Een van de voornemens uit de Agenda horizontale privacy is de start van publiekscommunicatie die burgers meer bewust moet maken van de

[1] Kamerstuk 34 926, nr. 8, p. 1.
[2] Idem, p. 6.

kst-34926-11
ISSN 0921 - 7371
's-Gravenhage 2021

privacyrisico's bij het gebruik van bijvoorbeeld digitale applicaties. De start van deze campagne, die aanvankelijk dit voorjaar zou plaatsvinden, heb ik tot begin volgend jaar uitgesteld.
De reden daarvoor is dat binnen het kabinet is afgesproken om publiekscampagnes, zolang de Coronacrisis dat vergt, te concentreren op onderwerpen die met deze crisis verband houden. Daarnaast heeft onderzoek plaatsgevonden naar de frequentie van horizontale privacyschendingen in zowel milde als ernstige vorm. Op basis van de uitkomsten daarvan wordt bekeken hoe de verschillende doelgroepen goed kunnen worden bereikt.

Omdat het geven van voorlichting over privacy en de bescherming van persoonsgegevens ook tot de wettelijke taak van de Autoriteit persoonsgegevens (AP) behoort, worden de activiteiten in het kader van de campagne nauw met haar afgestemd.

Om de boodschap langdurig en breder onder de aandacht te brengen is het voornemen om in 2021 de campagne te herhalen en de samenwerking met partners verder uit te bouwen.

Een ander speerpunt binnen het thema «voorlichting» vormt de voorlichting over de AVG aan het MKB. In mijn brief van 4 juni 2019 over de voorgenomen wijziging van de Uitvoeringswet AVG c.a. heb ik u al geïnformeerd over activiteiten die de AP op dat vlak heeft ontwikkeld en nog zal ontwikkelen.[3]

Herziening onderwijscurriculum

Met het oog op de bescherming van de privacy acht het kabinet het wenselijk dat kinderen al op jonge leeftijd leren verantwoord met sociale media om te gaan. Zoals uit de Agenda horizontale privacy blijkt, kan de lopende herziening van het curriculum voor het primair en voortgezet onderwijs daaraan een belangrijke bijdrage leveren. Bij deze herziening maakt een veilige en verantwoorde omgang met sociale media deel uit van het nieuwe leergebied «Digitale geletterdheid». In de kabinetsreactie op de herzieningsvoorstellen die de Minister voor Basis- en Voortgezet Onderwijs en Media op 9 december jl. aan de Tweede Kamer heeft aangeboden, heeft hij aangegeven dat er voor digitale geletterdheid een uitwerking ligt waarmee dit leergebied een goede plek in het curriculum kan krijgen.[4] Daarnaast werkt het Netwerk Mediawijsheid sinds 2008 aan het «mediawijzer» maken van de Nederlandse samenleving. Het Netwerk werkt daarbij samen met meer dan duizend netwerkpartners. Hier zijn ook organisaties bij aangesloten die betrokken zijn bij het onderwerp privacy. De website van het Netwerk Mediawijsheid, mediawijsheid.nl, biedt een breed publiek informatie over allerhande thema's omtrent het verstandig omgaan met digitale media.

2. Vergroting handelingsperspectief

Privacywijzer voor burgers en bedrijven

Een van de voorgenomen maatregelen om het handelingsperspectief voor burgers en bedrijven te vergroten was de ontwikkeling van een webportaal (de Privacywijzer) met praktische handreikingen die mensen helpen bij het uitoefenen van de rechten die zij op basis van de AVG hebben, en met hulpmiddelen voor bedrijven om aan de AVG te voldoen. In mijn brief van 31 oktober 2019 over voorgenomen wijzigingen van de

[3] Kamerstuk 32 761, nr. 164.
[4] Kamerstukken 31 293 en 31 289, nr. 495, p. 5 en 12.

Uitvoeringswet AVG heb ik u al bericht dat de ontwikkeling van de Privacywijzer is stopgezet. Gebleken was dat het webportaal «Hulpbij-privacy» van de AP inmiddels zo breed werd opgezet en zodanig werd ingericht dat het de functie van de toegezegde Privacywijzer kon overnemen.[5]

Laagdrempelige voorziening om privacyschendend beeldmateriaal van internet te verwijderen

In de Agenda horizontale privacy heeft het kabinet onderzoek naar een gebruiksvriendelijke voorziening voor burgers aangekondigd om onrechtmatige online content die tot hen te herleiden is, op een snelle wijze te laten verwijderen. Het onderzoek hiernaar is op 1 september jl. afgerond. De beleidsreactie op dit onderzoek stuur ik met deze brief mee.

Tijdens de plenaire behandeling van het burgerinitiatief internetpesten heb ik u ook toegezegd op Europees niveau aandacht te vragen voor het opnemen van een verplichting voor IT-platformen om onder bepaalde omstandigheden NAW-gegevens te verstrekken.[6] Inmiddels heeft de Europese Commissie aangekondigd dat de ecommerce Richtlijn zal worden herzien door middel van het zogenoemde Digital Services Act (DSA) pakket. Wat betreft het Nederlands standpunt verwijs ik u naar de kabinetsreactie op de gewijzigde motie van het lid Middendorp, die aan uw Kamer is aangeboden met de Geannoteerde Agenda van de Telecomraad van afgelopen juni[7] en naar de Geannoteerde Agenda van de Telecomraad van oktober jl. Een belangrijk uitgangspunt is dat de DSA moet bijdragen aan een sterke interne markt voor digitale diensten, de borging van publieke belangen en fundamentele rechten, en het voorkomen van administratieve lasten. Hierbij geldt dat fundamentele rechten die offline gelden, ook online moeten gelden. De DSA moet het tegengaan en bestrijden van illegale of onrechtmatige content, diensten en activiteiten ondersteunen. Ook moet er voldoende ruimte bestaan om in het kader van de opsporing en vervolging verplichtingen te kunnen opleggen aan de verschillende IT-platformen.[8]

Verbetering collectieve procedures

Het in de Agenda genoemde onderzoek naar verbetering van de mogelijkheden van het voeren van een collectieve actie tegen een schending van de privacy bij big-data-toepassingen heeft geresulteerd in een rapport van Tilburg University met als titel «De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving».[9] Op 20 november is de kabinetsreactie op een drietal onderzoeken naar algoritmen, waaronder het hiervoor genoemde onderzoek, aan de Tweede Kamer aangeboden.

3. Versterking normering

Strafbaarstelling wraakporno en seksuele intimidatie

Wraakporno kan een ernstige aantasting van de privacy opleveren. Met het oog daarop is sinds 1 januari jl. – mede ter uitvoering van het

[5] Kamerstuk 32 761, nr. 151, p. 1–2.
[6] Handelingen II 2019/20, 53, item 4, p. 11.
[7] Kamerstukken 21 501-33 en 25 295, nr. 812.
[8] Kamerstukken 21 501-33 en 25 295, nr. 812.
[9] https://www.wodc.nl/onderzoeksdatabase/2900-toetsingsmogelijkheden-van-big-data-toepassingen-bij-de-civiele-rechter.aspx.

regeerakkoord – misbruik van seksueel beeldmateriaal (wraakporno) zelfstandig strafbaar gesteld in artikel 139h van het Wetboek van Strafrecht.[10] Daarnaast is in mei van dit jaar een voorontwerp van het Wetsvoorstel seksuele misdrijven in consultatie gegeven, waarin strafbaarstelling van (online) seksuele intimidatie is opgenomen. Deze strafbaarstelling ziet op overlastgevend en opdringerig gedrag dat intimideren tot doel heeft. Het beoogt daarmee de (online) veiligheid van mensen verder te verbeteren.

Aanpak filmen van verkeersslachtoffers en andere hulpbehoevenden

Het fotograferen of filmen van verkeersslachtoffers en andere personen in hulpbehoevende toestand om deze beelden vervolgens online te delen, grijpt diep in op de privacy van betrokkenen en hun naasten.

Foto's en filmbeelden kunnen bijdragen aan het opsporen van strafbare feiten en het verklaren van ongelukken. Het delen van deze beelden leidt echter tot schade voor gefilmden of hun nabestaanden. Wanneer filmbeelden van ongevallen worden verspreid en online worden geplaatst, dan kan dit worden aangemerkt als een vorm van onrechtmatige online content. Over de wijze waarop onrechtmatige online content kan worden verwijderd, verwijs ik naar de bijgevoegde beleidsreactie.

Daarnaast is sinds 15 december 2019 het wederrechtelijk belemmeren van een hulpverlener gedurende de uitoefening van zijn beroep in zijn vrijheid van beweging strafbaar gesteld in artikel 426ter WvSr. Deze bepaling biedt de mogelijkheid repressief om op te treden tegen het hinderen van hulpverleners.

In dit verband verdient eveneens vermelding het initiatiefwetsvoorstel van de leden Van Toorenburg (CDA), Kuiken (PvdA) en Van den Berge (GroenLinks) dat de strafbaarstelling beoogt van de publicatie van beelden van personen die hulp behoeven of van overledenen. Dit voorstel is thans in internetconsultatie.

In de Agenda horizontale privacy heb ik een publiekscampagne aangekondigd om mensen op hun verantwoordelijkheid aan te spreken en de consequenties van hun handelen te laten inzien. Deze campagne zal deel uitmaken van de eerder in de brief genoemde campagne om het privacybewustzijn te vergroten. Zoals ik met betrekking tot die campagne al heb aangegeven, is deze campagne in verband met de Coronacrisis tot begin 2021 uitgesteld.

Aanscherping AVG in relatie tot de datamacht grote techbedrijven en profilering

Met betrekking tot de grote techbedrijven is in de Agenda horizontale privacy aangekondigd dat wordt onderzocht 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 heeft daarnaast willen inzetten op wettelijke voorschriften die specifieker zijn dan die in de AVG om risico's van profilering tegen te gaan bij bijvoorbeeld het aanbieden van producten en diensten. Zoals voorgenomen, heeft het kabinet dit onderdeel laten zijn van de evaluatie van de AVG.

[10] Wet van 27 september 2019 tot wijziging van onder meer het Wetboek van Strafrecht in verband met de herwaardering van de strafbaarstelling van enkele actuele delictsvormen (herwaardering strafbaarstelling actuele delictsvormen), Stb. 2019, nrs. 311 en 421.

In januari 2020 is de Raadspositie ten aanzien van de door de Europese Commissie uit te voeren evaluatie van de AVG vastgesteld.[11] Hierin benoemt de Raad dat de grote invloed van zogenoemde grote techbedrijven zorgen wekt. Daarbij is mede op verzoek van Nederland benoemd dat het zinvol is te onderzoeken of de AVG-rechten van betrokkenen met succes kunnen worden geëffectueerd jegens grote techbedrijven. Inmiddels is het evaluatieverslag van de Europese Commissie verschenen. Daarin benoemt de Commissie specifiek het belang van effectieve handhaving van de AVG jegens grote techbedrijven. Daarbij is het, naast het inzetten van alle tot toezichthouders beschikking staande handhavingsinstrumenten en het voldoende financieren van toezichthouders in de hele EU, essentieel dat er meer duidelijkheid komt over het samenwerkingsmechanisme van de toezichthouders en het toezicht op grensoverschrijdende verwerkingen. Ik steun deze oproep en bezie dan ook of de Nederlandse toezichthouder voldoende budget heeft om effectief toe te zien op de AVG.

Voorts geeft de Commissie aandacht aan het door Nederland aangebrachte punt over het effectueren van rechten, specifiek het recht op de overdraagbaarheid van gegevens. Indien met meer succes van dit recht gebruik gemaakt wordt, kunnen betrokkenen immers makkelijker overstappen naar andere aanbieders van (digitale) diensten. Ik ben zeer tevreden dat de Commissie zoveel nadruk legt op de noodzaak voor effectievere toepassing van dit recht in de digitale economie en dit koppelt aan aanstaande initiatieven die voortvloeien uit haar datastrategie.

Hoewel de Nederlandse zorgen doorklinken in het evaluatieverslag leidt dit niet tot een aanscherping van de bestaande normen. Dit kan worden bezien in de bredere context van het verslag, waarin de Commissie focust op de nadere uitwerking en handhaving van het bestaande kader. Bij brief van 4 december jl. (Kamerstukken 22 112 en 32 761, nr. 2994) heb ik uw Kamer mijn reactie gezonden op het evaluatieverslag AVG van de Europese Commissie

Waar het evaluatieverslag van de Commissie geen directe aanleiding biedt om normen aan te scherpen, constateer ik dat de datamacht van grote techbedrijven wordt geadresseerd in andere Europese trajecten, bijvoorbeeld op het gebied van mededinging. Voorts kan nog worden gewezen op het aankomende Europese initiatief ten aanzien van de DSA, waarin onder meer de verantwoordelijkheden van platforms nader wordt bezien. Het kabinet zal zich inspannen om in deze trajecten waar nodig verbindingen te leggen met de AVG en de fundamentele rechten die daarmee worden geborgd.

Wat betreft het aanscherpen van de wettelijke voorschriften om te voorkomen dat er met gebruik van algoritmen wordt gediscrimineerd bij het aanbieden van producten of diensten, heeft het kabinet in reactie op de motie van het lid Buitenweg[12] inzicht gegeven in hoe dergelijke discriminatie kan worden voorkomen. Kern daarvan is dat, hoewel dit specifieke onderwerp het evaluatieverslag van de Commissie niet heeft gehaald, het kabinet zich blijft inzetten om in Europees verband te bezien waar en in welke vorm extra transparantieverplichtingen nodig zijn. Concreet voorbeeld is de recente modernisering van het EU-consumentenrecht waarbij additionele informatieverplichtingen zijn geïntroduceerd voor de inzet van algoritmen bij het personaliseren van prijzen. Verder wijst het kabinet op de mogelijkheden om verdere regels voor bepaalde algoritmen, waaronder op het gebied van transparantie en

[11] https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf.
[12] Kamerstuk 32 761, nr. 138.

uitlegbaarheid, vast te stellen bij de uitwerking van Europese voorstellen op het gebied van Artificiële Intelligentie.[13]

Uit haar strategie voor de komende jaren, verwoord in «Focus AP 2020–2023», blijkt dat datamacht en profilering ook belangrijke prioriteiten van de AP zijn. In het focusgebied «datahandel» noemt de AP als aandachtsgebieden onder meer: toezicht op doorverkoop data, internet of things (zie ook hierna), profilering, en *behaviorial advertising*.[14] Het kabinet neemt de visie van de AP op deze punten uiteraard mee in de verdere beleidsontwikkeling.

Mededingingsbeleid in relatie tot online platforms

Om de ongewenste effecten tegen te gaan die het gevolg van marktmacht van sommige platforms kunnen zijn, zet het kabinet in op meer bevoegdheden voor een toezichthouder om op Europees niveau in te grijpen. Voor een toelichting op deze inzet verwijs ik naar de brief die de Staatssecretaris van Economische Zaken en Klimaat op 20 april jl. over dit onderwerp aan uw kamer heeft geschreven.[15] Daarnaast heeft de Europese Commissie op 15 december jl. het voorstel voor de «Digital Services Act» gepubliceerd, een vernieuwde basis voor digitale diensten.[16]

Inventarisatie risico's nieuwe technologische ontwikkelingen

In de Agenda horizontale privacy heeft het kabinet aangekondigd dat het wenselijk is om bij nieuwe technologische ontwikkelingen in een veel vroeger stadium na te denken over de risico's van deze ontwikkelingen voor de privacy van burgers. Tegen die achtergrond heeft het kabinet besloten onderzoek te laten doen naar de risico's van gezichtsherkenningstechnologie voor de privacy van burgers en naar de maatregelen die kunnen worden genomen om deze risico's te beperken. Dit heeft geresulteerd in een rapport van Tilburg University met als titel «Op het eerste gezicht: een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties». Dit rapport heb ik uw Kamer op 20 april jl. aangeboden. Daarbij heb ik de verwachting uitgesproken uw Kamer in het najaar een beleidsreactie op het onderzoek toe te zenden.[17] In deze beleidsreactie, die bij deze brief is gevoegd, onderstreep ik dat het verbod op de verwerking van bijzondere persoonsgegevens zoals biometrie, slechts onder strikte voorwaarden kan worden doorbroken. Om elke onduidelijkheid hierover weg te nemen, wordt in het wetsvoorstel tot wijziging van de Uitvoeringswet AVG (Verzamelwet gegevensbescherming) voorzien in een wijziging van artikel 29 van de UAVG. In de wettekst wordt expliciet opgenomen dat de uitzonderingsgrond van artikel 29 alleen kan worden toegepast wanneer dat nodig is voor een zwaarwegend algemeen belang. Met deze dubbele noodzakelijkheidstoets (noodzakelijk voor de authenticatie of beveiligingsdoeleinden én noodzakelijk omwille van een zwaarwegend algemeen belang), geeft de UAVG beter invulling gegeven aan de eis van artikel 9, tweede lid, onderdeel g, van de AVG De privacybescherming in het horizontale domein wordt daarmee versterkt.

---

[13] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[14] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf, p. 20–22.

[15] Kamerstuk 35 134, nr. 13.

[16] Zie https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.

[17] Kamerstuk 34 926, nr. 9.

Tot slot is vermeldenswaardig dat, op basis van de uitkomsten van de consultatie van het witboek kunstmatige intelligentie[18], de Europese Commissie doende is te onderzoeken of op dit gebied Europese regelgeving tot stand dient te komen.

Een andere ontwikkeling die de aandacht van het kabinet heeft getrokken, is het commercieel gebruik van DNA. Gebruik daarvan door iemand kan gegevens blootleggen over verwanten die daar niet om hebben gevraagd en dit ook niet wensen. Daarom onderzoek ik welke risico's dit gebruik voor de privacy van betrokkenen kan meebrengen en hoe deze risico's kunnen worden beperkt. Dit onderzoek vergt meer tijd dan aanvankelijk werd gedacht. Wel verwacht ik u in het eerste kwartaal volgend jaar over de uitkomst van dit onderzoek te kunnen informeren.

Beteugeling spyware

Als gevolg van technologische ontwikkelingen zijn producten waarmee gemakkelijk kan worden gespioneerd, goedkoper en makkelijker beschikbaar. Daarom heb ik in de Agenda horizontale privacy aangekondigd te laten onderzoeken of er in aanvulling op de al bestaande mogelijkheden in het strafrecht ook andere manieren zijn om spyware te reguleren en de risico's van het gebruik daarvan voor de privacy te verminderen. Daarbij zou ook het gebruik van hobbydrones worden betrokken. Een en ander heeft geresulteerd in een rapport van Tilburg University met als titel «Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden». Dit rapport heb ik uw Kamer op 23 juni jl. aangeboden (Kamerstuk 34 926, nr. 10). Daarbij heb ik de verwachting uitgesproken uw Kamer in het najaar een beleidsreactie op het onderzoek toe te zenden waarin ik inga op de verkende privacyrisico's en conclusies zal trekken met betrekking tot de onderzochte reguleringsopties. Voorts is 22 juli jl. door Tilburg University het rapport aangeboden «Het recht op privacy in horizontale verhoudingen». Daarin is onderzocht in hoeverre de situatie in Nederland zich verhoudt tot vier andere Europese landen, en of daaruit lering kan worden getrokken. De beleidsreactie op beide rapporten is gevoegd bij deze brief. Uiteraard is de AP bij de totstandkoming van deze beleidsreactie betrokken.

Ten aanzien van drones zal een belangrijke stap worden gezet met Verordening (EU) 2018/1139 van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart. Deze Verordening stelt scherpere voorwaarden aan het gebruik van drones, niet louter ten behoeve van de veiligheid en het milieu, maar ook uitdrukkelijk ter bescherming van de privacy van burgers. Onder de Verordening gelden meer voorschriften om drones te gebruiken en wordt een minimaal kennisniveau verplicht bij gebruik en wordt eenvoudiger herleidbaar aan wie een drone toebehoort. De Verordening laat ruimte aan lidstaten om ter bescherming van de privacy aanvullende regels vast te stellen. Mijn departement gaat hierover in het eerste kwartaal van 2021 met het Ministerie van Infrastructuur en Waterstaat in overleg. Ook zal mijn departement begin 2021 een privacyhandleiding voor het gebruik van drones publiceren. Deze informatie draagt bij aan bewustwording aan de zijde van de dronebestuurder en informeert de gedupeerden over de mogelijkheden die hen ten dienste staan.

[18] Kamerstukken 26 643 en 32 761, nr. 680.

Privacywaarborgen smart cities

De in de Agenda genoemde «Code goed digitaal openbaar bestuur» waaraan thans wordt gewerkt, zal mede van belang zijn voor bescherming van de privacy bij de verdere ontwikkeling van smart cities en de binnen dat concept bestaande relatie met burgers en bedrijven. Streven is de code in het eerste kwartaal van 2021 te publiceren.

De AP heeft onderzocht hoe privacywaarborgen en de bescherming van persoonsgegevens in de ontwikkeling en implementatie van smart city-toepassingen binnen Nederlandse gemeenten zijn vormgegeven. Het onderzoek heeft als doel om inzicht te verkrijgen in de kansen en risico's van smart city-toepassingen in relatie tot privacy. In de eerste fases van het onderzoek is gebleken dat de volwassenheid van de privacywaarborgen in gemeentelijke organisaties nog niet altijd op het gewenste niveau is. De bevindingen naar aanleiding van het onderzoek worden in het laatste kwartaal van 2020 gepubliceerd. De AP zal op basis hiervan aanbevelingen of *good practises* delen en *guidance* geven aan FG's en verantwoordelijken om de verdere ontwikkeling van privacyvriendelijke smart cities in Nederland te ondersteunen.
Daarnaast bestaat de wens bij de AP om de rol van gemeenten ten aanzien van private initiatieven inzake smart cities te verduidelijken.

Minimumveiligheidseisen IoT-apparaten

De koppeling van apparaten via het internet (IoT) kan, als de beveiliging niet goed is geregeld, ernstige inbreuken op de privacy veroorzaken. Zoals in de Agenda is beschreven, wordt op initiatief van Nederland in EU-verband onderzocht welke minimumveiligheidseisen via de Radio Equipment Directive (RED), die is geïmplementeerd in de Telecommunicatiewet, gesteld kunnen worden aan (draadloze) IoT-apparaten zoals smart watches en interactief speelgoed. Apparaten die niet aan de minimumeisen voldoen, kunnen dan van de markt worden geweerd en gehaald. In Nederland houdt het Agentschap Telecom toezicht op deze richtlijn. Verwacht wordt dat een daartoe benodigd besluit van de Europese Commissie uiterlijk in het voorjaar van 2021 wordt genomen, waarna met een overgangstermijn de genoemde minimumeisen zullen gaan gelden in de hele EU.

Ook de AP besteedt aandacht aan IoT-apparaten door met bedrijven en andere toezichthouders over de (privacy)eisen voor IoT-apparaten te spreken. Daarnaast heeft de AP in het afgelopen jaar tweemaal een informatieblad uitgebracht voor burgers waarmee zij de privacyrisico's van IoT-apparaten zelf kunnen verminderen. Dit is de handleiding «Connected car? Bescherm uw privacy!»[19] en de handleiding «Internet of Things en smart home? Bescherm uw privacy!»[20].

Financiële basis Autoriteit persoonsgegevens

Normering kan niet zonder toezicht en handhaving. De AVG heeft ingrijpende veranderingen meegebracht voor de Autoriteit Persoonsgegevens en haar toezicht. Inmiddels heeft de AP ervaring met de AVG opgedaan. In 2019 bedroegen de totale middelen die de AP van het ministerie heeft ontvangen € 20.492.000. Zoals in de brief «Taken en budgetontwikkeling AP» van 16 oktober 2019[21] is aangekondigd, laat ik

[19] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-connected-cars.
[20] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-internet-things-apparaten.
[21] Kamerstuk 32 761, nr. 149.

met de AP gezamenlijk een budgetonderzoek uitvoeren. Dit onderzoek is 2 november 2020 afgerond. Bij brief van 19 november jl. heb ik de eindrapportage met de resultaten van dit onderzoek aan uw Kamer aangeboden en daarbij de vervolgstappen geschetst.

4. Overige maatregelen

In de bijlage bij de Kabinetsvisie op de bescherming van de horizontale privacy zijn in reactie op de voorstellen uit de initiatiefnota «Onderlinge privacy» van het lid van uw Kamer Koopmans[22] eveneens maatregelen aangekondigd. Voor zover die niet al eerder in deze brief aan de orde zijn gekomen, wordt hierna de stand van zaken met betrekking tot de uitvoering van die maatregelen beschreven.

Faciliteren van online aangifte bij onderlinge privacy-schendingen

In de initiatiefnota werd onder meer bepleit om slachtoffers van onderlinge privacy-schendingen te faciliteren met de mogelijkheid om daarvan online aangifte te doen.
De mogelijkheid om online aangifte te doen beperkt zich op dit moment tot relatief eenvoudige delicten als diefstal, vernieling en oplichting. Hoewel deze mogelijkheid geleidelijk aan wordt uitgebreid, is het niet realistisch om te verwachten dat zij spoedig ook zal kunnen benut voor delicten op het vlak van onderlinge privacyschendingen, zoals wraakporno. Daarvoor is de context waarbinnen dergelijke delicten zich voordoen, veelal te complex. Wel werkt de politie aan een omnichannelstrategie waardoor men op meerdere manieren in contact kan komen met de politie.

Versterken van het recht op vergetelheid

Het voorstel in de initiatiefnota «Onderlinge privacy» om de uitoefening van recht op vergetelheid te versterken door het doen van aangifte mee te laten wegen in het urgent honoreren van een verzoek heeft geleid tot de volgende mededeling op de website van de AP: «Let op: heeft de verzoeker aangifte gedaan bij de politie tegen het delen van zijn of haar persoonsgegevens? Bijvoorbeeld in het geval van wraakporno? Overweeg dan of u het verzoek met meer urgentie kunt behandelen.»[23]

In de initiatiefnota werd ook gepleit voor de ontwikkeling van standaardprotocollen voor vergetelheidsverzoeken. Dergelijke protocollen zijn in de vorm van antwoorden op vragen die ondernemers zich kunnen stellen, opgenomen op de website van de AP.[24]

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. Vertegenwoordigers van mijn ministerie blijven daarom dan ook contact houden met vertegenwoordigers van het bedrijfsleven en organisaties die het privacybelang behartigen, om met elkaar van gedachten te wisselen over

[22] Kamerstuk 34 926, nr. 2.
[23] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#wat-moet-ik-als-organisatie-doen-als-ik-een-verzoek-krijg-om-gegevens-te-wissen-7228.
[24] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#wat-houdt-het-recht-op-vergetelheid-in-7261.

onderwerpen en ontwikkelingen die de bescherming van de onderlinge privacy raken. Daarbij zullen zij ook de AP blijven betrekken.

5. Slot

Aan het slot van de Agenda horizontale privacy is opgemerkt dat deze agenda kan worden aangevuld met nieuwe fenomenen, die voor een groot gedeelte terug te brengen zijn tot online privacy-schendingen en andere onrechtmatige gedragingen. Ook uw Kamer vraagt geregeld aandacht voor nieuwe fenomenen die de kop opsteken zoals *doxing*[25] en *deep nudes*[26]. Omdat het bij deze fenomenen in de kern ook steeds gaat om gedeeltelijk strafbare feiten, gedeeltelijk onrechtmatige handelingen en gedeeltelijk ongewenste gedragingen, kiest het kabinet ervoor om deze fenomenen steeds in de bredere context van de aanpak van illegale online content, onrechtmatige online content en ongewenste online content te bezien. Dat betekent dat ik – hoezeer ik ook de bezorgdheid van de Kamer over deze fenomenen deel – de focus wil leggen op de onderliggende mechanismen bij al deze fenomenen, om op die wijze het handelingsperspectief van slachtoffers te kunnen vergroten. De Agenda horizontale privacy zal, als daartoe aanleiding bestaat, te zijner tijd evenwel zeker van nieuwe onderwerpen worden voorzien.

De Minister voor Rechtsbescherming,
S. Dekker

[25] Kamervragen van de leden Groothuizen en Van Toorenburg nav het bericht «Meerdere OMT-leden bedreigd en thuis opgezocht», Aanhangsel Handelingen II 2020/21, nr. 1287.
[26] Motie van de leden Buitenweg en Van Toorenburg, Kamerstuk 35 570 VI, nr. 37.

Bijlage 1: **Beleidsreactie onderzoeksrapporten horizontale privacy**

Inleiding

Het WODC heeft drie onderzoeken gedaan op het terrein van privacy in horizontale verhoudingen.
Het eerste rapport «Het recht op privacy in horizontale verhoudingen», onderzoekt met name in hoeverre de situatie waarop in Nederland horizontale privacy is gewaarborgd, zich verhoudt tot andere Europese landen en of daaruit lering kan worden getrokken met het oog op de horizontale privacybescherming in Nederland. In het rechtsvergelijkende onderzoek zijn vier landen betrokken (Polen, Duitsland, Zweden en het Verenigd Koninkrijk).
Het tweede rapport, «Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden», zond ik op 23 juni jl. aan uw Kamer. In dit rapport is het resultaat te vinden van onderzoek naar producten waarmee gemakkelijk kan worden gespioneerd en die als gevolg van technologische ontwikkelingen goedkoper en makkelijker beschikbaar zijn. In het onderzoek is onder meer bezien in hoeverre de wet- en regelgeving zich verhoudt tot het spioneren met drones en met behulp van spionageapparatuur.
Het derde rapport, «Op het eerste gezicht, Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties» inventariseert het gebruik van gezichtsherkenningstechnologie en gaat in op inbreuken die daardoor kunnen worden gemaakt op de privacy en hoe dit kan worden voorkomen of beperkt.
Ik wil graag als volgt op deze rapporten reflecteren.

Privacy in horizontale verhoudingen: rechtsvergelijkend onderzoek

De onderzoekers concluderen dat de horizontale privacy in Nederland en de onderzochte landen op een min of meer gelijke wijze is gereguleerd. In zowel Nederland als in de onderzochte landen is de horizontale werking van grondrechten onderkend. Wat daarbij een belangrijke rol speelt, naast het EVRM, is de Algemene Verordening gegevensbescherming die in alle genoemde landen van kracht is. De onderzoekers komen tot de slotsom dat de horizontale werking van grondrechten in de onderzochte landen weinig uiteenlopen met het stelsel in Nederland.
In strafrechtelijk opzicht bestaan tussen de onderzochte landen (accent)-verschillen. De rechtsvergelijking wijst niet op hiaten in de strafrechtelijke normering van horizontale privacy schendingen in Nederland. Ik merk daarbij op dat het Wetboek van Strafrecht nog onlangs (sinds 1 januari jl. met de Wet herwaardering strafbaarstelling actuele delictsvormen, Stb. 2019, nr. 311) is herzien, mede naar aanleiding van voortschrijdende technologische ontwikkelingen. Bij deze herziening is mede gekeken in hoeverre meer gedragingen die de persoonlijke levenssfeer aantasten onder de strafwet dienen te vallen en daarbij de keuze gemaakt om strafbaarstelling te beperken tot specifieke gedragingen. Op dit punt wordt hieronder verder teruggekomen in het kader van het gebruik van spionageproducten en drones.

Spioneren met hobbydrones en andere technologieën

Het onderzoek «Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden» is nagegaan in hoeverre het bestaande pakket aan wet- en regelgeving toegesneden is op de aanpak van schendingen van de persoonlijke levenssfeer die door middel van spionageproducten plaatsvindt. Onderzocht is of de bestaande wettelijke instrumenten

aanvulling behoeven, en of er ook andere manieren zijn om deze te reguleren.

In het onderzoek wordt een tweedeling gemaakt tussen spionageproducten in enge zin (apparaten die in de eerste plaats zijn ontworpen of aangepast voor het heimelijk verzamelen van informatie over personen) en spionageproducten in brede zin (apparaten die kunnen worden gebruikt om heimelijk informatie over een persoon te verzamelen, maar waarvan een dergelijke heimelijke verzameling van informatie niet het hoofddoel is van ontwerp of gebruik). Voorbeelden van de eerste categorie zijn minicamera's, een pen met ingebouwde afluisterapparatuur, en locatietrackers (zowel fysieke apparaten als spyware). Smartphones en hobbydrones met camera's zijn voorbeelden van de tweede categorie.

Ten aanzien van spionageproducten in brede zin wil ik met name ingaan op drones. Een belangrijke ontwikkeling op dit terrein is de Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart (hierna: de Verordening), die voorwaarden stelt aan het gebruik van drones. De Verordening onderkent uitdrukkelijk dat onbemande luchtvaartuigen risico's kunnen vertegenwoordigen voor niet alleen de veiligheid en het milieu, maar ook voor de privacy van burgers en de bescherming van hun persoonsgegevens. De Verordening stelt daarom eisen aan de registratie van drones en aan de gemakkelijke toegankelijkheid van die registratiegegevens. Onder de Verordening worden drones ingedeeld in categorieën, afhankelijk van de veiligheidsrisico's. Hoe meer risico's, hoe meer voorschriften er gelden. Anders gezegd: de mate van certificering, registratie, verzekering en vergunningsverplichting hangt af van de categorie waar de drone in valt en het risico van de operatie die met de drone wordt uitgevoerd. Uitzonderingen op de registratieplicht zijn drones uit de open categorie, die minder wegen dan 250 gram.
Een voorbeeld van het handelingsperspectief dat hierdoor ontstaat bij inbreuken op de privacy, is dat drones die onder de werking van de Verordening vallen voorzien dienen te zijn van een uitleesbare tag. In deze tags staat alle informatie over de drone, wie de exploitant is en een registratienummer. Dit maakt eenvoudiger traceerbaar aan wie een drone toebehoort en of deze voldoet aan de vereisten en of in overeenstemming wordt gehandeld met de AVG. Verwacht wordt dat hiervoor wel nadere fysieke controle vereist is.
De Verordening maakt dat de drempels voor het gebruik van drones worden verhoogd, dat dronevliegers een minimaal kennisniveau behoren te bezitten en dat bij een schending van de regels en/of bij een inbreuk op de privacy, eenvoudiger herleidbaar is aan wie de drone toebehoort. Zowel de dronebestuurder als de persoon die geschaad wordt, vallen beiden onder de waarborgen van de AVG.
Verder laat de Verordening ruimte aan lidstaten om, met het oog op openbare veiligheid of bescherming van de privacy en persoonsgegevens, nationale regels vast te stellen waarin nadere voorwaarden worden verbonden aan het gebruik van drones. Wanneer van deze ruimte gebruik zal worden gemaakt, zal uw Kamer hierover vanzelfsprekend worden geïnformeerd.
Om de bewustwording van dronegebruikers te vergroten worden drone piloten tijdens hun opleiding bekend gemaakt met de regels, onder andere op het gebied van privacy. Eveneens in het kader van bewustwording zal het Ministerie van Justitie en Veiligheid begin 2021 een privacy handleiding drones publiceren waar informatie over privacy risico's bij dronevluchten staat vermeld. Deze informatie draagt bij aan bewustwording aan de zijde van de dronebestuurder en informeert de gedupeerden over de mogelijkheden die hen ten dienste staan.

Daarnaast zullen de Ministeries van Justitie en Veiligheid en van Infrastructuur en Waterstaat in het eerste kwartaal van 2021 in onderling overleg de noodzaak en mogelijkheden bezien of de Verordening drones voldoende handvatten biedt op het vlak van privacy en veiligheid en, indien dat niet het geval is, op welke wijze aan de hand van nadere regels daaraan invulling kan worden gegeven.

Zoals gezegd is in het rapport ook onderzoek gedaan naar spionageproducten in enge zin. Aan de dat de wetgeving substantiële bescherming biedt tegen schendingen van de privacy door middel van een spionageproduct, hecht ik veel waarde. Het kabinet ziet zich immers regelmatig gesteld voor de vraag in hoeverre ontwikkelingen in de samenleving ertoe nopen om wettelijke normen bij te stellen. Dit geldt niet in de laatste plaats voor technologische ontwikkelingen, wanneer daardoor de gelegenheid kan ontstaan om, soms ernstige, inbreuken te maken op het privéleven van anderen. Dit vraagt om voortdurende aandacht.
De Wet tot wijziging van onder meer het Wetboek van Strafrecht in verband met de herwaardering van de strafbaarstelling van enkele actuele delictsvormen (herwaardering strafbaarstelling actuele delictsvormen, wet van 27-09-2019, Stb. 2019, nr. 311) illustreert dat het kabinet oog heeft voor veranderende maatschappelijke opvattingen mede naar aanleiding van technologische ontwikkelingen. Die kunnen ertoe leiden dat gedragingen die veel onrust en leed veroorzaken niet louter als laakbaar, maar tevens als strafwaardig dienen te worden aangemerkt. Dit maakt niet alleen in voorkomende gevallen een repressieve aanpak mogelijk, maar draagt ook bij bewustwording en normbesef.
Bij de totstandkoming van de Wet herwaardering strafbaarstelling actuele delictsvormen was het kabinet zich er bewust van dat digitalisering van de samenleving leidt tot een toename van mogelijkheden om beeldmateriaal te vervaardigen en te verspreiden. Dit kan een aantasting van de persoonlijke levenssfeer tot gevolg hebben. Daarbij heeft het kabinet ervoor gekozen om niet iedere aantasting, hoe onwenselijk soms ook, onder de werking van de wet te brengen maar om de strafbaarstelling af te bakenen tot de meest evidente privacy schendingen. Het gaat dan om het zonder medeweten en/of toestemming van tot stand brengen van seksueel beeldmateriaal en het openbaar maken van seksueel beeldmateriaal om de afgebeelde persoon schade te berokkenen. Dergelijk handelen kan grote (psychische) gevolgen voor en impact op slachtoffers hebben en is derhalve bij genoemde wet als misdrijf strafbaar gesteld. Een strafbaarstelling van élke vervaardiging of openbaarmaking van beeldmateriaal, zelfs wanneer de afgebeelde daardoor in een compromitterende situatie wordt gebracht, ziet het kabinet als dermate ruim dat deze op gespannen voet kan komen te staan met het legaliteitsbeginsel en de vrijheid van meningsuiting. Deze afweging maakt dat op dit moment de aanleiding ontbreekt voor opnieuw een herziening van strafbepalingen.
Ten aanzien van de in het onderzoek voorgestelde verbodsbepalingen stel ik voorop dat – op Europees noch nationaal niveau – niet snel wordt overgegaan tot verbodsbepalingen op apparaten, gezien het belang vanuit vrije marktwerking. Een verbod kan worden overwogen wanneer dat nodig zou zijn ter bescherming van de openbare orde of de openbare veiligheid, of als daarmee een zwaarwegend maatschappelijk belang is gediend. Dan zal bovendien moeten zijn gebleken dat er geen minder zwaarwegende alternatieven voorhanden zijn. Op dat punt verkeren we op dit moment niet met de in het onderzoeksrapport gemeld producten. Het gaat om producten die geen illegaal gebruiksdoel hebben en waarvan het enkele bezit of gebruik nog geen inbreuk veroorzaakt op de rechtsorde of de gerechtvaardigde belangen van derden. Wanneer een bezitter te kwader trouw is, en het product wordt gebruikt als hulpmiddel om een strafbaar feit te plegen, kan het uit het verkeer worden genomen door bijvoorbeeld inbeslagneming en verbeurdverklaring. Voor algehele

verbodsbepalingen ontbreekt naar het oordeel van ik derhalve de noodzaak.
De onderzoekers bepleiten voorts een gelijke benadering van fysieke en softwarematige locatietracering, omdat bij fysieke locatietracking (bijvoorbeeld het plaatsen van een zender onder een auto) niet snel voldaan is aan de delictsbestanddelen van artikel 350 WvSr, terwijl het plaatsen van trackingsoftware op een computer of smartphone al gauw strafbaar is op grond van artikel 350a WvSr. Tussen beide strafbepalingen zit echter geen incongruentie; zij beschermen hetzelfde rechtsgoed en stellen – in essentie – vernieling of beschadiging strafbaar. Artikel 350a Sr ziet daarbij op handelingen die het functioneren van informatiesystemen raken, bijvoorbeeld waardoor de vertrouwelijkheid en beschikbaarheid van gegevens of de integriteit van systemen, programmatuur en diensten kan worden aangetast. Geen van beide strafbepalingen beoogt de privacy schending als zodanig strafbaar te stellen.
Het vorenstaande laat vanzelfsprekend onverlet dat, afhankelijk van de context, tegen inbreuken op de persoonlijke levenssfeer kan worden opgetreden door de meer algemene strafbaarstellingen die de wet kent, zoals gebruik van een verborgen camera, smaad, laster, belediging en/of bedreiging. Een ieder kan bovendien melding doen van onrechtmatige of strafbare inhoud op internet opdat deze wordt verwijderd en wanneer dat niet gebeurt, aangifte doen van een strafbaar feit. De officier van justitie kan vervolgens een bevel afgeven tot verwijdering van de strafbare content. Ik verwijs in dit verband tevens naar de beleidsreactie op het onderzoek naar een laagdrempelige voorziening om privacy schendend beeldmateriaal van internet te verwijderen, waarin het bestaan van een gebruiksvriendelijke voorziening om onrechtmatige online content snel te laten verwijderen, centraal staat.

Tegen de achtergrond van het voorgaande volgt geen noodzaak het (onlangs herziene) strafwettelijk kader opnieuw tegen het licht te houden voor spionageproducten in enge zin. Dit geldt mutatis mutandis ook voor de bestaande regels buiten het strafrecht, zoals de in het onderzoek genoemde AVG en de APV's, binnen de kaders waarvan het evenmin vrijelijk geoorloofd is om met behulp van spionageproducten heimelijk persoonsgegevens, waaronder beeldmateriaal te verzamelen en te verspreiden.
Tot slot valt de inzet van een drone of ander hulpmiddel als voorverkenning voor het plegen van een ernstig strafbaar feit, reeds onder het bereik van de strafbaarstelling van voorbereidingshandelingen. Daaronder is begrepen het voorhanden hebben van voorwerpen of informatiedragers bestemd tot het begaan van het misdrijf. Voor een verruiming van de strafbare voorbereiding naar misdrijven waarop een lagere dan de thans vereiste gevangenisstraf is gesteld, zie ik onvoldoende aanleiding.

Op het eerste gezicht: onderzoek naar gezichtsherkenning

Het onderzoeksrapport »Op het eerste gezicht, Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties» is uitgevoerd door de Universiteit van Tilburg in opdracht van het WODC (Ministerie van Justitie en Veiligheid). In het onderzoek wordt het gebruik van gezichtsherkenningstechnologie geïnventariseerd, wordt beschreven hoe dit inbreuk kan doen op de horizontale privacy van burgers en worden handvatten gegeven om inbreuken op de privacy te voorkomen of beperken. Met dit onderzoek is uitvoering gegeven aan de motie van de leden Verhoeven en Van Dam (Kamerstuk 35 300 VI, nr. 64).
Gezichtsherkenningstechnologie wordt ingezet om op basis van digitale beelden (bijvoorbeeld een foto of video), gezichten of gezichtskenmerken te herkennen. Het rapport richt zich op gezichtsherkenningstechnologie in horizontale relaties: relaties tussen bedrijven en burgers en tussen

burgers onderling. Gezichtsherkenningstoepassingen in horizontale relaties bevinden zich in Nederland nog in de experimentele fase en richten zich voornamelijk op de volgende doelen, zoals gemak en efficiëntie (snelle check-in bij evenementen); beveiliging en controle (autorisatie en onwenselijk gedrag tegen gaan); personalisatie en proactieve dienstverlening (commerciële nudging).

Zoals het onderzoek vaststelt, is de AVG het belangrijkste juridische handvat om gezichtsherkenningstechnologie te reguleren. Biometrische gegevens die personen (uniek) identificeren zijn volgens de AVG bijzondere persoonsgegevens waarvan de verwerking in beginsel verboden is. Op dit verbod kunnen slechts onder strikte voorwaarden uitzonderingen worden gemaakt. Verwerking kan zijn toegestaan als er uitdrukkelijke toestemming is van de betrokkene of als de camera's met gezichtsherkenning worden ingezet voor beveiligings- en authenticatiedoeleinden om een zwaarwegend algemeen belang te dienen.
Toestemming dient duidelijk, actief en in vrijheid te zijn gegeven; er mag geen twijfel over bestaan dat toestemming is verleend. Dit zal in de praktijk geen reële grond vormen voor een uitzondering op het verwerkingsverbod, omdat in redelijkheid niet kan worden verwacht dat iedereen die een ruimte betreedt waar gezichtsherkenning wordt toegepast, daarvoor expliciete toestemming geeft.
Daarnaast maakt artikel 9, tweede lid, onderdeel g, van de AVG het mogelijk om een uitzondering te maken op het verbod om biometrische gegevens te verwerken indien de verwerking noodzakelijk is om «redenen van zwaarwegend algemeen belang». Op grond van artikel 29 UAVG geldt zo'n uitzondering, wanneer dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden. In het wetsvoorstel Verzamelwet gegevensbescherming wil ik de aanvullende eis opnemen dat per geval een dubbele noodzakelijkheidstoets plaatsvindt; de verwerking moet noodzakelijk zijn om redenen van zwaarwegend algemeen belang èn voor authenticatie of beveiligingsdoeleinden. Als zwaarwegend algemeen belang, de eerste noodzakelijkheidstoets, kan bijvoorbeeld worden gedacht aan het beschermen van de volksgezondheid, het voorkomen van milieuschade of het beveiligen van vitale processen. Ten aanzien van authenticatie en beveiligingsdoeleinden, de tweede noodzakelijkheidstoets, speelt de vraag of het doel van de verwerking in verhouding staat tot de inbreuk op de privacy van de betrokkenen (proportionaliteit) en of het doel niet op een andere manier kan worden bereikt die minder ingrijpend is voor de betrokkenen (subsidiariteit). Wanneer een uitzondering op het verwerkingsverbod kan worden gemaakt, gelden alle vereisten van de AVG ten aanzien van de verwerking. Daarmee ligt de lat hoog voor het verwerken van biometrische persoonsgegevens.
Het naleven van de voorwaarden die uit de AVG voortvloeien is temeer van belang, nu gezichtsherkenning in de praktijk een onzichtbare digitale techniek is. Bij gezichtsherkenning wordt een beeldbestand opgenomen met een reguliere camera geanalyseerd door een algoritme. Het onderscheid tussen camerabewaking en gezichtsherkenning is dan ook niet te maken op basis van de zichtbare hardware. Daarbij worden biometrische persoonsgegevens bij gezichtsherkenning zodanig afgenomen dat dit niet waarneembaar is voor de persoon in kwestie. Daardoor kan gezichtsherkenning onbewust (en ook achteraf) plaatsvinden.

Gelet op het voorgaande is gezichtsherkenning in horizontale relaties in principe
niet toegestaan. Gezichtsherkenningstoepassingen maken immers gebruik van bijzondere persoonsgegevens waarvan de verwerking in beginsel verboden is. Dat brengt met zich mee dat in de relatie tussen burgers onderling in beginsel geen ruimte bestaat voor het gebruik van gezichtsherkenningstechnologie. Ook in de relatie tussen burger en bedrijven of

organisaties geldt dat de AVG zeer weinig ruimte biedt om gezichtsherkenning in te zetten. Wanneer daartoe toch wordt overgegaan, moet de verwerkingsverantwoordelijke verantwoording afleggen dat aan de in de artikel 9 in samenhang bezien met 29 UAVG genoemde voorwaarden wordt voldaan en dat daarnaast de juiste organisatorische en technische maatregelen zijn genomen. Identificatie door middel van biometrie zal eerder noodzakelijk en proportioneel kunnen zijn op plekken waar gevaarzetting voor de publieke veiligheid of gezondheid kan ontstaan wanneer onbevoegden zich daar toegang weten te verschaffen, dan wanneer het gaat om publieke ruimten.
Een totaalverbod voor het gebruik van gezichtsherkenningstechnologieën zou naar mijn oordeel toegevoegde waarde ontberen, nu de AVG reeds het verwerken van bijzondere persoonsgegevens verbiedt. Voor die gevallen waarin een uitzondering op het verwerkingsverbod denkbaar is, zie ik niet aanstonds dat het in de AVG opgenomen instrument van de voorafgaande raadpleging voor deze vorm van verwerking tekortschiet. Immers, wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren en de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, dan is de verwerkingsverantwoordelijke gehouden tot een voorafgaande raadpleging van de AP. De AP geeft dan advies over de omgang met de risico's van de voorgenomen verwerking. Ik zal de werking van dit instrument in relatie tot het verwerken van biometrische gegevens betrekken bij de evaluatie van de UAVG en in de gesprekken met de AP.

Een en ander neemt niet weg dat de ontwikkelingen op dit terrein steeds zullen voortgaan. Het is belangrijk om hier scherp en bedacht op te blijven en te blijven bezien onder welke voorwaarden deze technologieën eventueel kunnen worden toegepast. Het is echter minstens zo belangrijk dat burgers en bedrijven doordrongen zijn van de kwetsbaarheden en risico's. Zoals voor vele deze technologische ontwikkelingen, geldt ook hier dat bewustwording van burgers en bedrijven van groot belang is om duidelijk te maken welke gevaren en juridische (en mogelijkerwijs ook sociale en ethische) grenzen er zijn aan het toepassen van gezichtsherkenningstechnologieën. Dit vraagt om voortdurende investeringen in de bewustwording. Ik reken het tot mijn taak om aan die bewustwording een bijdrage te leveren.

Slot

Ten aanzien van spionageproducten in brede zin waaronder drones, zal de Verordening drones bijdragen aan verbeterde regulering en toezicht, wat ook zal bijdragen aan een betere bescherming van de privacy. Ik bezie nog in hoeverre de Verordening aanvullende nationale privacyregelgeving behoeft. In dit verband zal nauwe samenwerking met het Ministerie van Infrastructuur en Waterstaat worden gezocht om nader naar de aanvullende nationale regelgeving te kijken. In het kader van bewustwording zal bovendien een privacyhandleiding voor gebruikers van drone worden gepubliceerd.

Verder onderschrijf ik de vaststelling van de onderzoekers dat het wettelijk kader voldoende is toegerust wanneer het gaat om spionageproducten in enge zin, op de meest ingrijpende schendingen van de persoonlijke levenssfeer. Een bredere strafbaarstelling voor het openbaar maken of toezenden van informatie zou weliswaar meer mogelijkheden bieden om horizontale privacy schendingen tegen te gaan, maar daardoor kunnen weer andere rechten onder druk komen te staan. Op dit moment zie ik derhalve geen reden voor verdere uitbreiding van strafbaarstellingen. De balans om zowel de uitingsvrijheid en informatievrijheid in een vrije samenleving te respecteren alsook om ernstige schendingen van de

privacy aan te pakken, is naar mijn oordeel in de huidige wetgeving voldoende aanwezig. Het rapport geeft dan ook geen aanleiding om met nieuwe regelgeving te komen voor spionageapparatuur in enge zin.
Wel onderken ik dat handhaving van de regelgeving niet altijd gegeven is. Ik zal de ontwikkelingen op dit vlak blijven volgen.
De meeste winst bij het tegengaan van privacyschendingen door spionageapparatuur valt, gelet op het vorenstaande, te halen in het verbeteren van het normbesef en bewustwording.
Met de onderzoekers deel ik de conclusie dat wet- en regelgeving niet de enige instrumenten zijn om privacy in horizontale verhoudingen te reguleren. Dit past in de kabinetsvisie op de bescherming van de horizontale privacy, zoals uiteengezet op 7 juni 2019 (Kamerstuk 34 926, nr. 8, p. 1). Bij brief waar deze reactie een bijlage bij is, is uw Kamer nader geïnformeerd over de stand van zaken rond de uitvoering van de maatregelen die in deze agenda zijn genoemd.

Bijlage 2:

Beleidsreactie onderzoek «Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content»

Op 11 november jl. is het onderzoek «Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content» openbaar gemaakt.[27] Het kan niet zo zijn dat het zonder toestemming plaatsen van privacy-gevoelige informatie of afbeeldingen op het internet, alsmede andere vormen van het plaatsen van onrechtmatige content ongestraft blijft, ik ben daarom blij met de concrete handvatten die het onderzoek biedt om onrechtmatige content snel verwijderd te krijgen en te borgen dat slachtofferschap niet blijft voortduren. Het is mijn wens om op dit onderwerp een stap naar voren te doen.

Het kabinet zet de komende tijd in op een traject waarbij:
Stap 1: het kabinet duidelijk positie kiest in de discussie rond een nieuwe Europese Digital Services Act, waarbij Nederland inzet op een verplichting aan providers en internetplatformen om actief mee te werken aan het opsporen en verwijderen van strafbare en anderszins onrechtmatige content. *(Planning: gereed eerste helft 2021)*;
Stap 2: het kabinet met betrokken partijen nadere uitwerking en invulling geeft aan bestaande Notica-and-Take-Action en Notice-and-Take-Down-procedures, zodat content snel en accuraat van het internet gehaald kan worden na een melding daarover. *(Planning: gereed eind 2021)*;
Stap 3: het kabinet met uitvoeringsinstanties en toezichthouders concrete afspraken maakt over de beoordeling van content en de handhaving van verwijderverzoeken. *(Planning: gereed voorjaar 2022)*;
Stap 4: het kabinet – waar nodig – het stelsel van meldpunten en toezichthouders stroomlijnt en aanvult met een civielrechtelijke procedure. *(Planning: vanaf 2022)*.
Met deze voorgestelde aanpak neemt het kabinet – ook in internationaal en Europees perspectief – een vlucht naar voren ten aanzien van de aanpak van onrechtmatige online content. Deze aanpak zal deels internationaal, deels Europees en deels nationaal invulling krijgen. Nederland steunt daarbij de positie van de Europese Commissie dat de tijd van vrijwillige en vrijblijvende zelfregulering voorbij is: Mensen moet een weerwoord worden geboden tegen de uitwassen en misstanden op internet en socialemediaplatformen.

Afbakening

Dit onderzoek gaat over onrechtmatige content. De beleidsreactie is een aanvulling op het kabinetsbeleid om strafbare gedragingen als *hate speech*, kinderporno en terroristische content online tegen te gaan (deze vormen van content worden aangeduid met de term illegale content), maar ook op het beleid en aanzien van ongewenste content (zoals verschillende verschijningsvormen van desinformatie). In dit onderzoek gaat het over content waarbij sprake is van schade in een relatie tussen burgers onderling. Meestal geschiedt dat door een horizontale privacy-schending (het zonder toestemming delen van afbeeldingen of persoons-gegevens). Een voorbeeld dat in deze context veel wordt gebruikt is het op internet delen van non-consensuele naaktbeelden. We kijken daarbij in eerste instantie naar het bestuursrecht (privacy-schending) en naar het civielrecht (onrechtmatige daad). Daarbij onderscheidt het zich van content die in strijd is met het wetboek van strafrecht.

[27] Voor de belangrijkste bevindingen van het onderzoek verwijs ik u naar de aanbiedingsbrief die op 2 december 2020 naar uw Kamer is gezonden (Kamerstuk 34 602, nr. 6).

Vorm	Rechtsbasis om op te treden	Interventies
Illegale content	Wetboek van Strafrecht	Verwijdering, vervolging
Onrechtmatige content	*Burgerlijk Wetboek; Algemene Verordening Gegevensbescherming*	*Verwijdering, schadevergoeding/boete*
Ongewenste content	Geen	O.a. fact checking, counter speech

Omdat zowel bij illegale content als bij onrechtmatige content het verwijderen daarvan het primaire doel is, overlappen de instrumenten die daartoe kunnen worden ingezet deels met die om illegale content als kinderpornografie en terroristische content tegen te gaan. Ook juridisch lopen de termen in elkaar over: een strafbare gedraging is immers ook altijd onrechtmatig. Toch is het van belang om steeds goed voor ogen te hebben over welke vorm van online content we het hebben (illegaal, onrechtmatig of ongewenst), omdat op deze verschijningvormen van online content verschillende rechtsgebieden van toepassing zijn, die allemaal hun eigen specificiteit hebben. Met vier stappen, hieronder nader toegelicht, wil ik een nieuw evenwicht realiseren in de verhouding tussen burgers en internetbedrijven voor wat betreft onrechtmatige content. Zo wil ik komen tot een effectieve en efficiënte manier van de aanpak van deze content.

Stap 1: Europees voorstel Digital Services Act (DSA)

Op 14 december heeft de Europese Commissie haar voorstel voor een Digital Services Act (DSA) gelanceerd. De DSA zal ook een nieuwe versie van de Richtlijn Elektronische Handel (REH) (2000/31/EG) omvatten. De onderzoekers constateren dat een aantal aspecten van de REH een effectief verwijderingsbeleid van onrechtmatige content bemoeilijkt. De onderhandelingen over de DSA bieden een uitgelezen mogelijkheid om deze aspecten nog eens tegen het licht te houden. Specifiek gaat het daarbij om het creëren van een specifiek rechtskader over de rol, verantwoordelijkheid en eventuele aansprakelijkheid voor internetplatformen (naast internetaanbieders en hostingbedrijven). Notice-and-Take-Down of Notice-and-Take-Action (NTD/NTA)voorschriften kunnen daar een onderdeel van zijn. De DSA biedt ook de mogelijkheid om een aantal uitgangspunten uit reeds bestaande Gedragscodes te codificeren en verdere invulling te geven.
Tegelijkertijd zal nieuwe Europese wetgeving ervoor moeten zorgen dat fundamentele rechten en publieke belangen worden geborgd zodat consumenten en bedrijven worden beschermd. Daarnaast geldt dat fundamentele rechten die offline gelden, ook online moeten gelden. Dit betreft bijvoorbeeld de mogelijkheid om bezwaar aan te tekenen tegen een verwijderbesluit, maar ook de termijn waarbinnen een melding moet worden afgehandeld. De herziening van de DSA moet het tegengaan en bestrijden van illegale of onrechtmatige content, diensten en activiteiten ondersteunen. Daarbij is het van belang om fundamentele rechten, zoals privacy en vrijheid van meningsuiting te beschermen en tegelijkertijd te zorgen voor veiligheid en cybersecurity.
In de geannoteerde agenda bij de Telecomraad van 26 mei 2020 heeft de Staatssecretaris van Economische Zaken en Klimaat in antwoord op de motie van het lid Middendorp aangegeven wat we belangrijk vinden in relatie tot de DSA.
Daartoe behoort ook dat gebruikers een effectieve en laagdrempelige manier moeten hebben om bezwaar te maken tegen illegale of anderszins

onrechtmatige informatie of tegen de verwijdering van informatie die zij hebben geplaatst.[28]

Stap 2: Het nader invulling geven aan Europese en nationale NTD- en NTA-procedures

Indien de DSA een nieuw kader zet voor de rol en verantwoordelijkheid van platformen, dan moeten de bestaande NTD- en NTA-procedures ook tegen het licht worden gehouden en daarmee in lijn gebracht. Daarbij horen duidelijke afspraken over wie bepaalt dat online content het predicaat strafbaar of onrechtmatig krijgt en in aanmerking komt voor verwijdering, en op basis van welke criteria dat gebeurt. Ook de reikwijdte en afdwingbaarheid van de NTD-procedures zijn van belang. Zo zou het streven moeten zijn dat ook de internetplatformen zich aansluiten bij Europese en nationale NTD- en NTA-procedures. Dit zou idealiter gepaard moeten gaan met een verplichting voor relevante internetdiensten tot uniforme informatievoorziening over beschikbare procedures tot verwijdering. Tenslotte moet er aandacht zijn voor de uitwerking van het land-van-oorsprong-beginsel in de praktijk, in die zin dat het een effectieve rechtshandhaving niet in de weg staat en dat er een mogelijkheid blijft bestaan om op nationaal niveau aanvullende regulering te instigeren. Voor het kabinet blijft zelfregulering daarbij het uitgangspunt, maar waar dit tot obstakels in de handhaving en opsporing leidt, zal het niet aarzelen ook door te pakken en te kiezen voor (co-)regulering van overheidszijde. Een intermediair-functie tussen overheid en platformen kan worden vervuld door zgn. «trusted flaggers», die objectief kunnen vaststellen of content naar de juridische maatstaven zoals die in Nederland gelden als onrechtmatig moet worden beschouwd en vervolgens een verwijderverzoek kunnen doen. Van belang is ook, dat bezwaar aangetekend kan worden tegen een besluit tot verwijdering van content. In dat kader zal ik een verkenning laten uitvoeren naar alternatieve geschillenbeslechting met betrekking tot het vaststellen van de rechtmatigheid van online content.

Stap 3: De Autoriteit Persoonsgegevens (AP) nadere invulling laten geven aan «onrechtmatige content»

Providers en platformen geven aan behoefte te hebben aan normering. Ze zijn – enkelen nagelaten – over het algemeen bereid mee te werken om strafbare en anderszins onrechtmatige content te bestrijden, maar dan moet wel duidelijk zijn, welke uitingen als strafbaar of onrechtmatig aangewezen kunnen worden. Een aantal platformen heeft ervoor gekozen deze begrippen voor het eigen platform verder uit te werken. Dat neemt niet weg dat vrijwel alle providers en platformen content hosten die naar Nederlandse maatstaven als strafbaar of onrechtmatig kan worden gekwalificeerd en dat er tussen de providers en platformen onderling grote verschillen bestaan ten aanzien van hun verwijderbeleid en het bewust of onbewust niet ingrijpen om verdere verspreiding van de content te voorkomen. Voor mij staat als een paal boven water dat het niet zo kan zijn dat platformen eigen regels hanteren die ruimte bieden aan strafbare of anderszins onrechtmatige uitingen op het internet. Daartegenover geldt dat platformen weliswaar het recht hebben zelf te bepalen of zij bepaalde vormen van content willen weigeren die noch strafbaar, noch anderszins onrechtmatig is (bijvoorbeeld consensuele naaktbeelden), maar dat daarbij wel steeds aandacht moet zijn dat de vrijheid van meningsuiting niet onnodig wordt beperkt.
Bij onrechtmatige uitingen is het toetsingskader veelal de onrechtmatige daad (artikel 6:162 BW), dan wel het bestuursrecht. Het kan niet van

[28] Kamerstukken 21 501-33 en 25 295, nr. 812.

platformen verlangd worden dat zij steeds de juiste afwegingen maken in het vaststellen of een uiting al dan niet onrechtmatig is. Naar mijn mening van het kabinet ligt er een taak bij de AP om via haar oordelen een standaard te ontwikkelen voor rechtmatige online content. Ik zal met de AP in gesprek gaan en in beeld brengen wat er nodig is om de AP invulling te laten geven aan deze taak.

Stap 4: Experiment met kortgedingprocedure voor onrechtmatige content die buiten het strafrecht en de werking van de AVG valt

Voor het melden van strafbare content (kinderporno, discriminatie/hate speech, terroristische content) zijn meldpunten ingericht. Over onrechtmatige content die een (horizontale) privacyschending betreft kan de AP oordelen. Voor onrechtmatige content die niet in één van deze categorieën valt staan diverse civiele procedures open.
Ik ben het met de onderzoekers eens dat civiele procedures een uiterste redmiddel zijn als het gaat om verwijdering van onrechtmatige online content (de route van een NTD/NTA-procedure zal altijd sneller en eenvoudiger zijn). Aangezien de onderzoekers verder concluderen dat de bestaande civiele procedures op zich toereikend zijn en zij verschillende andere mogelijkheden opperen om de positie van benadeelden te verbeteren, ligt het voor de hand om primair in te zetten op deze andere mogelijkheden. Dat neemt niet weg dat ik de suggestie om voor dit soort zaken met een kantonrechterskortgeding te experimenteren interessant vind. Daarom zal ik – indien daar na uitwerking van de andere in deze brief genoemde sporen nog een noodzaak toe blijft bestaan – een experiment opzetten, waarbij onrechtmatige content aanhangig gemaakt kan worden via een kantonrechterskortgeding.

Routekaart, mediacampagne en steunpunt

Uit het onderzoek komt een grote behoefte naar voren aan het verduidelijken van online rechten waar mensen een beroep op kunnen doen en van de juiste route(s) om die rechten te kunnen uitoefenen. Om hieraan tegemoet te komen zal ik als sluitstuk van de te nemen maatregelen vanaf de tweede helft van 2022 een routekaart opstellen, met een compleet overzicht van alle mogelijkheden die benadeelden ten dienste staan. Maar eerst bouw ik voort op bestaande initiatieven – private en van overheidswege – om voorlichting aan benadeelden te geven over hun rechten op internet en manieren waarop zij die rechten kunnen uitoefenen. Zo laat ik naast de campagne een steunpunt voor belanghebbenden inrichten. De onafhankelijkheid van een dergelijk meldpunt of kenniscentrum en de betrokkenheid van reeds bestaande onafhankelijke toezichthouders met taken op het gebied van onrechtmatige online content zijn daarbij belangrijke aandachtspunten. Tevens zal ik in beeld laten brengen welke kosten gepaard gaan met het inrichten van een dergelijk steunpunt. Op het moment dat de routekaart gereed is, naar verwachting eind 2022, zal ik inzetten op het in brede kring bekend maken daarvan, bijvoorbeeld door een actieve mediacampagne.

Tijdspad en financiën

Om de bovenstaande stappen te verwezenlijken is tijd nodig. Ik besef dat het tijdspad de huidige kabinetsperiode zal overschrijden. Bovendien heeft het kabinet op de Europese besluitvorming rond de DSA niet de eindregie in handen. Het zal ook aan een volgend kabinet zijn om uiteindelijk te komen tot het opzetten van een steunpunt en daarvoor de benodigde financiële middelen vrij te maken.