# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2021–2022 **Aanhangsel van de Handelingen**


**Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden**

## 2367

Vragen van het lid **Rajkowski** (VVD) aan de Ministers van Economische Zaken en Klimaat en van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de beantwoording van de vragen «Litouwen adviseert consument geen Xiaomi-telefoons meer te kopen»* (ingezonden 9 november 2021).

Antwoord van Minister **Adriaansens** (Economische Zaken en Klimaat), mede namens de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 7 april 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 891.

Vraag 1
Hoe weet u zeker dat op de smartphones geen censuur wordt toegepast en dat deze software constant uit staat, aangezien u in de beantwoording aangeeft dat er op de in de Europese Unie verkochte smartphones geen censuur wordt toegepast, er voor Nederland op dit moment geen aanleiding is om een dergelijk zwaarwegend advies af te geven en dat u ziet dat het daadwerkelijk toepassen van dergelijke software inbreuk kan maken op de grondrechten van gebruikers?

Antwoord 1
Het Ministerie van Defensie van Litouwen heeft onderzoek gedaan naar telefoons van het merk Xiaomi. Daarbij is ook gekeken naar de functionaliteit die in deze vragen wordt aangeduid als censuursoftware. Uit het onderzoek blijkt dat deze functionaliteit is uitgeschakeld in de Europese Unie. Naar aanleiding van het Litouwse onderzoek heeft ook het Duitse *Bundesambt für Sicherheit in der Informationstechnik* (BSI) een eigen onderzoek ingesteld. Daarbij zijn geen bijzonderheden aangetroffen.[1] In beide onderzoeken is vastgesteld dat de software in de praktijk niet wordt toegepast. Ik hecht eraan dat dit ook in de toekomst niet zal gebeuren.
Gebruikers van telefoons moeten immers met elkaar kunnen communiceren zonder dat er, zoals zou gebeuren als de bedoelde functionaliteit wordt geactiveerd, door derden inbreuk wordt gemaakt op de communicatie. Dit zogenoemde communicatiegeheim is onder meer vastgelegd in artikel 5 van richtlijn 2002/58/EG (de e-privacyrichtlijn) en ook in het voorstel voor een

[1] German IT security watchdog: No evidence of censorship function in Xiaomi phones | Reuters


ah-tk-20212022-2367
ISSN 0921 - 7398
's-Gravenhage 2022

Europese e-privacyverordening die in de toekomst de e-privacyrichtlijn zal vervangen.
Zolang de e-privacyverordening nog niet van kracht is, is een complicerende factor dat artikel 11.2a van de Telecommunicatiewet waarin artikel 5 van de e-privacyrichtlijn is omgezet, zich alleen richt tot aanbieders van openbare elektronische communicatienetwerken en diensten en dus niet tot derden zoals de leverancier van de telefoon. Omdat de totstandkoming van de e-privacyverordening nog op zich laat wachten, zal ik nader bezien of het doelmatig is om de Telecommunicatiewet op dit punt aan te passen.
Naast de Telecommunicatiewet wordt het communicatiegeheim ook beschermd in het Wetboek van Strafrecht. Zo stelt artikel 139c het met een technisch hulpmiddel aftappen of opnemen van het telecommunicatieverkeer strafbaar. Betoogd zou kunnen worden dat het met software bekijken (aftappen) en vervolgens aanpassen (het er uit filteren van «ongewenste» zoekresultaten) van het telecommunicatieverkeer onder de werking van deze strafbepaling valt (vgl. Hoge Raad, 17 december 2019, ECLI:NL:HR:2019:1973). In dat geval zou het activeren van dergelijke software ertoe kunnen leiden dat sprake is van een strafbaar feit.
Waar apparaten bijvoorbeeld de zoekresultaten filteren, dan kan dit voorts een inbreuk vormen op de vrijheid van nieuwsgaring. Het is uiteindelijk aan de rechter om in voorkomende gevallen een uitspraak te doen over de rechtmatigheid van zo'n filter.

Vraag 2
In hoeverre worden er, in het kader van «Bring-Your-Own-Device», privé Xiaomi-telefoons gebruikt, waarvan in de beantwoording is aangegeven dat er sinds 2018 60 van zijn aangeschaft, en is dit wenselijk?

Antwoord 2
Voor «Bring-Your-Own-Device» binnen de rijksoverheid geldt als uitgangspunt dat ieder rijksonderdeel moet aangeven of en in welke gevallen het gebruik van eigen apparatuur is toegestaan op basis van een eigen risicoafweging. De (on)wenselijkheid hiervan verschilt dus per rijksonderdeel. Mocht het gebruik van eigen toestellen toegestaan zijn dan geldt, net zoals voor overheidstoestellen, dat op basis van de risicoafweging de juiste maatregelen worden getroffen om de overheidsinformatie voldoende te beschermen, bijvoorbeeld door toepassing van cryptografische oplossingen die op het eigen apparaat gebruikt kunnen worden.
In antwoord op eerdere vragen is aangegeven dat er zover bekend bij het Ministerie van Binnenlandse Zaken sinds 2018 60 Xiaomi telefoons zijn aangeschaft binnen de rijksoverheid. Deze zijn aangeschaft om te worden gebruikt als onderwerp van technisch, forensisch of opsporingsonderzoek. Er is geen relatie tussen deze 60 telefoons en «Bring-Your-Own-Device»-beleid.

Vraag 3
In hoeverre biedt de Baseline Informatiebeveiliging Overheid voldoende handvatten om nieuwe informatie en potentiële risico's zoals censuursoftware zoveel als mogelijk te voorkomen?

Antwoord 3
De Baseline Informatiebeveiliging Overheid (BIO) is een informatiebeveiligingskader voor de hele overheid en is gebaseerd op de internationale standaarden ISO27001 en ISO27002. De BIO kent een risicogebaseerde aanpak. Dat betekent dat overheidsorganisaties op basis van risicoafweging (nieuwe) dreigingen onderkennen en daarop passende en proportionele beveiligingsmaatregelen treffen. Zo ook deze casus.
De BIO kent (nog) geen specifieke maatregelen tegen dergelijke software. Dit jaar wordt de BIO geëvalueerd. Onderdeel van die evaluatie is de herijking van de dreigingen die richting geven aan de concrete overheidsmaatregelen in de BIO. Dit vraagstuk zal daarbij worden meegenomen.
In algemene zin geldt dat eind 2018 ten aanzien van nationale veiligheidsrisico's een verscherpt inkoop- en aanbestedingsbeleid is geïmplementeerd voor de rijksoverheid. Hierin is opgenomen dat bij inkoop en aanbesteding mogelijke risico's voor de nationale veiligheid per inkoopopdracht worden meegewogen. Bij de aanschaf en implementatie van gevoelige apparatuur of programmatuur wordt volgens dit beleid rekening gehouden met zowel

risico's in relatie tot een leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld als het gaat om de toegang tot systemen door derden.
Ter ondersteuning van dit beleid is aanvullend instrumentarium ontwikkeld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen.
In het Commissiedebat Digitale overheid, datagebruik en algoritmen, en digitale identiteit van 22 maart jl. heeft de Staatssecretaris voor Koninkrijksrelaties en Digitalisering verder toegezegd een onderzoek te gaan doen naar inkoopeisen en -richtlijnen over cyberveiligheid in het overheidsapparaat, dat voornamelijk zal gaan over landen met een offensief cyberprogramma. In het daaropvolgende tweeminutendebat van 29 maart is in aanvulling op de toezegging een motie ingediend door Kamerleden Rajkowski en Van Weerdenburg, om in dit onderzoek ook te kijken naar de vitale sector.[2] De motie is op 5 april aangenomen; de Kamer zal over het vervolg geïnformeerd worden.

Vraag 4
Wat zou u ervan vinden als Rijksambtenaren Chinese censuursoftware zouden downloaden op hun apparaten?

Antwoord 4
In algemene zin is het onwenselijk als rijksambtenaren software zouden downloaden op hun werkapparaten als die een conflict zou opleveren met hun werkzaamheden.
Verder wil ik opmerken dat de werkomgeving van rijksambtenaren op mobiele apparaten zich bevindt op een afgeschermd deel dat niet toegankelijk is voor overige geïnstalleerde software.

Vraag 5
Onderkent u dat Xiaomi telefoons, in tegenstelling tot wat er in de beantwoording te lezen is, niet alleen via verschillende webwinkels verkocht worden, maar dat er sinds 2020 ook een fysieke «Mi-store» is geopend in Rotterdam, de eerste fysieke Xiaomi winkel in de Benelux?

Antwoord 5
In de eerdere beantwoording is aangegeven dat Xiaomi-toestellen in Nederland breed verkrijgbaar zijn. Het klopt dat er een fysieke Xiaomi-winkel in Rotterdam is.

Vraag 6
Hoe beoordeelt u het feit dat aanbieders van apparaten waar censuursoftware op staat winkels openen in Nederland en hun marktaandeel in Nederland groeiend is?

Antwoord 6
Het is belangrijk dat producten die hier op de markt worden gebracht voldoen aan de relevante regelgeving. Dat wordt des te belangrijker als het een wijdverspreid product is. Tegelijkertijd is het iedereen die zich aan de relevante Nederlandse en Europese wetgeving houdt toegestaan producten op de Nederlandse en Europese markt te brengen.

Vraag 7
Klopt het dat de censuursoftware op afstand kan worden geactiveerd vanuit China, zonder dat gebruikers dit doorhebben? Deelt u de mening dat deze functionaliteit een potentiële bedreiging vormt voor de vrijheid van menings-

[2] Kamerstukken vergaderjaar 2021/22, 26 643, nr. 839

uiting en de vrije toegang tot informatie van Nederlandse gebruikers van Xiaomi-toestellen? Zo ja, hoe beoordeelt u dit? Zo nee, waarom niet?

Antwoord 7
Een fabrikant kan op afstand wijzigingen doorvoeren aan producten en diensten door software-updates uit te brengen. Op basis van artikel 11.7a van de Telecommunicatiewet moet de fabrikant daarover de eindgebruiker informeren en bovendien diens toestemming verkrijgen voor de wijziging.
De vrije nieuwsgaring wordt onder meer beschermd door artikel 10 van het Europees Verdrag voor de Rechten van de Mens. Hiervoor is het van belang dat mensen degelijke toegang hebben tot informatie zonder hierin te worden gehinderd. De gigantische hoeveelheid informatie die in de moderne wereld voorhanden is maakt het echter noodzakelijk dat technische hulpmiddelen zoals zoekmachines deze informatie filteren voordat het aan gebruikers wordt voorgelegd. Voor vrije nieuwsgaring is het van belang dat deze filtering waardenvrij plaatsvindt.
Het is onwenselijk voor gebruikers om heimelijk af te worden gehouden van specifieke onderwerpen. Uit zowel het Litouwse als Duitse onderzoek blijkt echter dat dit in de Europese Unie op Xiaomi telefoons ook niet wordt gedaan. Het is in het algemeen belangrijk dat gebruikers de beperkingen van hun apparatuur kennen en begrijpen en indien zij dat wensen kunnen kiezen uit alternatieve browsers en zoekmachines om te voorzien in hun informatiebehoefte.

Vraag 8
Hoe beoordeelt u het feit dat ook de data van Nederlandse gebruikers die Xiaomi-toestellen gebruiken wordt doorgestuurd naar Xiaomi-servers in China, waar conform de geldende Chinese cyberveiligheidswet, ook de Chinese overheid toegang heeft tot de data van Nederlandse gebruikers?

Antwoord 8
Nederland en de EU spreken in verschillende verbanden, waaronder binnen de VN, met China over dataveiligheid. Centraal hierbij staat de bescherming van privacy, zoals de naleving van de Algemene verordening gegevensbescherming (AVG), bescherming van mensenrechten en het tegengaan van ongepaste toegang van overheden tot datagegevens. Zoals aangegeven in de Notitie «Nederland-China: Een nieuwe balans» (Kamerstuk 35 207, nr. 1) staat het kabinet achter striktere handhaving en sterker uitdragen van bestaande standaarden en normen, zoals de Europese regelgeving op het gebied van data, bescherming van persoonsgegevens en privacy en productveiligheid. Partijen moeten, wanneer zij in de EU producten of diensten aanbieden, voldoen aan de vereisten die conform het gegevensbeschermingsrecht op hen rusten. In dit geval zijn deze vereisten primair neergelegd in het algemene kader dat de AVG biedt voor de verwerking van persoonsgegevens en de speciale regels uit de Telecommunicatiewet. De AVG kent een ruim toepassingsbereik. Artikel 3, tweede lid, onder a AVG bepaalt dat verwerkingsverantwoordelijken die goederen of diensten aanbieden aan betrokkenen in de EU binnen het toepassingsbereik vallen. De AVG bepaalt onder meer dat er een «rechtsgrondslag» moet zijn om persoonsgegevens te verwerken (bijvoorbeeld toestemming), dat betrokkenen geïnformeerd moeten worden over de verwerking van hun gegevens en dat zij in staat worden gesteld om de rechten uit te oefenen die zij over hun gegevens hebben.
Voor zover het gaat om gegevens die worden afgelezen van het randapparaat van de eindgebruiker (ook als dit geen persoonsgegevens zijn) is artikel 11.7a van de Telecommunicatiewet van toepassing. Dit ook bij vraag 7 genoemde artikel bepaalt dat voor het plaatsen en aflezen van informatie op een randapparaat de toestemming van de eindgebruiker noodzakelijk is. Voor een rechtsgeldige toestemming is van belang dat de eindgebruiker adequaat is geïnformeerd over de doeleinden van de gegevensverzameling en verwerking. Op deze bepaling wordt toezicht gehouden door Autoriteit Consument en Markt (ACM).
In algemene zin geldt dat, wanneer persoonsgegevens naar een land buiten de Europese Unie worden doorgegeven, er additionele voorwaarden gelden. Doorgifte is namelijk slechts toegestaan op grond van een van de wettelijke bepalingen uit hoofdstuk V van de AVG. Aangezien voor China geen door de Europese Commissie genomen adequaatheidsbesluit bestaat, waarin wordt

besloten dat dit land een passend beschermingsniveau waarborgt, kan structurele doorgifte van persoonsgegevens alleen plaatsvinden voor zover er door de verwerkingsverantwoordelijke «passende waarborgen» worden geboden.
Het is aan de Autoriteit Persoonsgegevens (AP), de toezichthouder op de AVG, om erop toe te zien dat er passende waarborgen zijn getroffen. Als dit niet het geval is heeft de AP onder meer de bevoegdheid om boetes op te leggen, maar ook om de verwerking te verbieden.

Vraag 9
Klopt het dat de Belgische Staatsveiligheidsdienst al eerder publiekelijk heeft gewaarschuwd voor spionage via Chinese spionage, waaronder die van Xiaomi? Zo ja, hoe beoordeelt u dit en deelt u de mening dat deze waarschuwing zeer zorgelijk is?

Antwoord 9
Het klopt dat de Belgische Staatsveiligheid heeft gewaarschuwd voor potentiële Chinese spionagedreiging. Zoals ook staat beschreven in het Dreigingsbeeld Statelijke Actoren (DBSA)[3] en de jaarverslagen van de inlichtingen- en veiligheidsdiensten is toenemende afhankelijkheid van buitenlandse technologie een gegeven. Hierdoor bestaat het risico dat met technologische toeleveringen de digitale spionage- en sabotagemogelijkheden toenemen. Waar dit de nationale veiligheid raakt, wordt per geval afgewogen welke maatregelen proportioneel zijn om dit risico te beheersen. Risico's voor de nationale veiligheid kunnen met name ontstaan wanneer technologie de Nederlandse vitale infrastructuur of gevoelige kennis en informatie raakt.

Vraag 10
In hoeverre is de huidige aangewezen toezichthouder in staat om te controleren of er censuursoftware op mobiele telefoons aanwezig is en of deze software daadwerkelijk actief is?

Antwoord 10
De toekomstige e-privacy verordening bevat regels over (de verwerking van persoonsgegevens bij) elektronische communicatie om te zorgen dat de persoonlijke levenssfeer wordt beschermd. Daarin wordt het controleren van de communicatie, ook door leveranciers van telefoons, verboden. Als de verordening van kracht wordt of voorafgaand daaraan de Telecommunicatiewet wordt aangepast conform het gestelde onder vraag 1, is er pas een aangewezen toezichthouder op dit punt.
Voor zover de vraag gaat over het in staat zijn om te controleren of er een betreffende functionaliteit op mobiele telefoons aanwezig is en of deze actief is, komt uit de genoemde onderzoeken bij vraag 1 naar voren dat dit het geval is. Uit die onderzoeken bleek dat de functionaliteit in de praktijk niet wordt toegepast.

Vraag 11
Hoe beoordeelt u de aanwezigheid van censuursoftware op Xiaomi-toestellen in het kader van een eerdere uitspraak, gedaan door de Algemene Inlichtingen- en Veiligheidsdienst, dat er sprake is van een «wereldwijde grootschalige vergaring van persoonsgegevens door Chinese actoren om profielen te maken van medewerkers van bedrijven en instellingen waar het land digitaal wil inbreken»?

Antwoord 11
De betreffende functionaliteit ziet op het detecteren en blokkeren van bepaalde termen. Deze functionaliteit heeft geen verband met grootschalige vergaring van persoonsgegevens. Zie het antwoord op vraag 1 ten aanzien van deze functionaliteit en het antwoord op vraag 8 ten aanzien van dataveiligheid.

[3] Kamerstuk 30 821, nr. 124

Vraag 12
Deelt u de mening dat het zeer onwenselijk is dat ook de telefoons van Nederlandse gebruikers deze software kunnen bevatten en dat er een mogelijkheid is dat de censuursoftware wordt geactiveerd? Zo ja, bent u bereid een onafhankelijk onderzoek te laten uitvoeren door bijvoorbeeld het Agentschap Telecom en de Nationaal Coördinator Terrorismebestrijding en Veiligheid naar de mogelijke aanwezigheid van deze censuursoftware op Xiaomi-toestellen die in Nederland worden verkocht? Zo nee, waarom niet?

Antwoord 12
Ik zie geen noodzaak tot het doen van een aanvullend onderzoek naar de in het artikel genoemde software op Xiaomi-toestellen. Wel zal ik nader bezien of het doelmatig is om de Telecommunicatiewet op dit punt aan te passen. Zie hiervoor het antwoord op vraag 1.
Daarnaast is, zoals ook in de hoofdlijnenbrief digitalisering van 8 maart jl. aangegeven, digitaal bewustzijn noodzakelijk. We investeren samen met de ministeries van Justitie en Veiligheid en Binnenlandse Zaken en Koninkrijksrelaties in het vergroten van kennis onder burgers over digitale veiligheid en over technologische ontwikkelingen, zodat zij zich bewust zijn van de mogelijkheden, beperkingen, kansen en risico's van technologie. Op de website veiliginternetten.nl wordt voorlichting en handelingsperspectief gegeven over het veilig gebruik van een apparaat.