Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

32 761 Verwerking en bescherming persoonsgegevens

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 303

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 juni 2024

In de procedurevergadering van de vaste commissie voor Digitale Zaken van 20 december 2023 is gesproken over het artikel «De online advertentie-industrie bedreigt de nationale veiligheid» van Follow The Money d.d. 18 december 2023.[1]
De commissie heeft het kabinet verzocht een reactie op dit artikel te geven.
Op 16 januari jl. heeft het lid Six Dijkstra (NSC) mondelinge vragen gesteld aan de Minister van Justitie en Veiligheid, bij afwezigheid van de Minister voor Rechtsbescherming, over het artikel «Nederlandse telefoons online stiekem te volgen: «Extreem veiligheidsrisico»» van BNR. De Minister van Justitie en Veiligheid heeft toen toegezegd op de gestelde vragen te zullen terugkomen in een brief. In de petitie «Bescherm Nederlandse burgers tegen online tracking» is vervolgens opnieuw aandacht gevraagd voor de brede maatschappelijke gevolgen over de handel in persoonsgegevens.[2]

Met deze brief geven wij invulling aan de verzoeken en informeren wij uw Kamer over de lopende acties. Allereerst wordt in deze brief de kern van de artikelen weergegeven. Daarna gaan wij in op de aanpak van het kabinet, de relevante wet- en regelgeving en het toezicht op de naleving daarvan. Tot slot bespreken wij de risico's voor de nationale veiligheid en de bevoegdheden van de inlichtingen- en veiligheidsdiensten.

[1] Online advertentiedata bedreigt nationale veiligheid | Follow The Money.
[2] Petitieaanbieding «Bescherm Nederlandse burgers tegen online tracking».

kst-32761-303
ISSN 0921 - 7371
's-Gravenhage 2024

Kern van de artikelen en petitie

De artikelen van Follow The Money[3] en BNR[4] beschrijven de handel in en de gevolgen van de grote hoeveelheden (ofwel: *bulk*) persoonsgegevens die op de online advertentiemarkt zijn verkregen. De betrokken onderzoeksjournalisten konden door datasets te combineren Nederlandse burgers, militairen, politici, politieagenten, en medewerkers van inlichtingen- en veiligheidsdiensten identificeren en hun verplaatsingen volgen. Ook konden hun gegevens eenvoudig worden gekoppeld aan andere gevoelige informatie over persoonlijke situatie, voorkeuren en problemen. De artikelen beschrijven de inbreuk die dit maakt op de privacy van betrokkenen en de kwetsbaarheid die dit veroorzaakt op het vlak van spionage, chantage, en beïnvloeding door zowel statelijke als niet-statelijke actoren.

Zoals toegezegd aan uw Kamer, zullen wij in deze brief ingaan op (1) het wettelijk stelsel voor de bescherming van persoonsgegevens, (2) het potentiële risico van grootschalige gegevensverzameling voor de nationale veiligheid en (3) de bevoegdheden van de inlichtingendiensten bij het opkopen van online-advertentie gegevens voor «OSINT»-onderzoeken.

1. Wettelijk stelsel voor gegevensbescherming

Het kabinet is zich bewust van de zorgen zoals die zijn geuit in recente artikelen over de risico's die de online advertentie-industrie kan opleveren voor burgers en de nationale veiligheid. Wij vinden het onwenselijk als persoonsgegevens in strijd met het gegevensbeschermingsrecht worden verwerkt en online verhandeld. Het wettelijke kader van de Algemene Verordening Gegevensbescherming (AVG) speelt bij de gegevensbeschermingsvraagstukken van de online advertentie-industrie een essentiële rol.

In het hiernavolgende bespreken wij allereerst kort enkele hoofdlijnen van het wettelijk kader van de AVG en de rechten van betrokkenen daarin, de rol van de verwerkingsverantwoordelijke bedrijven die handelen in persoonsgegevens, het toezicht- en handhaving op de naleving van regelgeving, het belang van bewustwording en verantwoordelijkheid bij online-surfgedrag, en tot slot enkele aanvullende maatregelen die het kabinet neemt. Hiermee beantwoorden wij de vragen die uw Kamer hierover heeft gesteld.

Wettelijk kader gegevensbescherming

De kern van de uitwerking van het gegevensbeschermingsrecht in de Europese Unie (EU) wordt gevormd door de AVG.[5] De AVG stelt regels en voorwaarden aan de verwerking van persoonsgegevens. Die regels zijn onverminderd van toepassing bij de verkoop van persoonsgegevens via online veilingen.[6] Een van die regels is dat iedere gegevensverwerking rechtmatig moet zijn, hetgeen betekent dat daarvoor een geldige grondslag, zoals toestemming van betrokkene of gerechtvaardigd belang, moet zijn. Toestemming voor het verwerken van persoonsgegevens zoals bedoeld in de AVG dient steeds vrij, voor een specifieke verwerking en een specifiek doel, goed geïnformeerd, en ondubbelzinnig te zijn gegeven. Als persoonsgegevens zijn verzameld op basis van toestemming, is verdere verwerking buiten de gebieden die vallen onder de oorspronke-

---

[3] «De online advertentie-industrie bedreigt de nationale veiligheid» - Follow the Money.
[4] Nederlandse telefoons online stiekem te volgen: «Extreem veiligheidsrisico» – BNR.
[5] Algemene Verordening gegevensbescherming (EU) 2016/679
[6] *Kamerstukken II* 2022–2023, 32 761, nr. 286

lijke toestemming of de wettelijke bepaling, niet mogelijk. Voor verdere verwerking is dan nieuwe toestemming of een andere rechtsgrondslag noodzakelijk.

Tijdens het mondelinge vragenuur op 16 januari 2024 vroeg uw Kamer welke rechten betrokkenen hebben op grond van de AVG. Het gaat dan om de rechten van degenen wiens persoonsgegevens worden verwerkt jegens een verwerkingsverantwoordelijke, de partij onder de AVG die verantwoordelijk is voor de verwerking van persoonsgegevens. Deze rechten zijn bedoeld om te zorgen dat mensen in beginsel moeten kunnen nagaan waar hun persoonsgegevens worden verwerkt.[7] Zo heeft een betrokkene bijvoorbeeld het recht op inzage op de verwerkte persoonsgegevens (artikel 15 AVG) en op rectificatie (artikel 16 AVG) daarvan. Daarnaast heeft een betrokkene het recht op gegevenswissing (artikel 17 AVG), op beperking van de verwerking (artikel 18 AVG), en bezwaar (21 AVG). Zo heeft de burger de mogelijkheid om gegevensverwerkingen die in de ogen van betrokkene onrechtmatig zijn, aan te vechten. Deze rechten hangen dan ook nauw samen met de bepalingen in de AVG die betrekking hebben op het toezicht en de rechtsbescherming. Naast gebruik van het recht op schadevergoeding kan betrokkene melding maken bij de Autoriteit Persoonsgegevens (AP) of een verzoekschriftprocedure starten bij de rechter.

Het kabinet ziet dat de AP klachten ontvangt over organisaties die niet of te laat reageren op een inzageverzoek. De komende tijd gaat de AP samen met andere privacytoezichthouders onderzoeken in hoeverre organisaties de regels voor het recht op inzage naleven. Dit onderzoek is een gezamenlijk project van de Europese privacytoezichthouders, het Europees Comité voor gegevensbescherming (de EDPB). De EDPB zal de resultaten van deelnemende landen bundelen en daarover rapporteren.[8] Tegelijkertijd ziet het kabinet dat betrokkenen toestemming kunnen geven voor gegevensverwerkingen zonder zich van de gevolgen daarvan goed bewust te zijn. Gelet op het belang van gegevensbescherming en de nadelige gevolgen voor burgers en andere betrokkenen is dit onwenselijk. Daarom wil het kabinet, zoals reeds eerder in de Kamerbrief over cookies en online tracking die door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken mede namens de Minister voor Rechtsbescherming is toegezegd aan uw Kamer, het bewustzijn bij burgers over de verzameling van persoonsgegevens door mobiele applicaties en websites vergroten.[9]

Laatste stand van zaken rondom cookies en tracking

Naast de AVG is er de ePrivacyrichtlijn[10] die betrekking heeft op de bescherming van privacy en persoonlijke gegevens binnen de sector van elektronische communicatie. In deze richtlijn staan specifieke voorschriften voor cookies. Zoals is uiteengezet in de Kamerbrief cookies en online tracking heeft het kabinet zich ingespannen om de regels op Europees niveau te verbeteren. Het huidige kabinet vindt dat het mogelijk moet zijn om gemakkelijker cookies en andere vormen van online tracking te kunnen weigeren. Op die manier zijn gebruikers beter in staat hun privacy te beschermen.

---

[7] H.R. Kranenborg & L.F.M. Verhey, *De Algemene verordening gegevensbescherming in Europees en Nederlands perspectief (Mastermonografieën staats- en bestuursrecht)*, Deventer: Kluwer 2018, p. 191 e.v.

[8] CEF 2024: Launch of coordinated enforcement on the right of access | European Data Protection Board (europa.eu)

[9] *Kamerstukken II* 2022–2023, 32 761, nr. 286.

[10] Richtlijn - 2002/58 - EN - EUR-Lex (europa.eu)

Verantwoordelijkheden internationale bedrijven

In het vragenuur van 16 januari 2024[11] kwam de verantwoordelijkheid van grote internationale bedrijven die via Real-time bidding (RTB)-gegevensprofielen van personen opstellen aan de orde. Deze bedrijven zijn in het licht van de AVG veelal de verwerkingsverantwoordelijke of verwerker, en daarmee, verantwoordelijk voor naleving van de AVG. Daarbij hoort ook dat die bedrijven de nodige passende technische en organisatorische maatregelen nemen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Onlangs heeft het Hof van Justitie van de Europese Unie (HvJEU) nog de regels verduidelijkt die uit de AVG voortvloeien voor online veilingen van persoonsgegevens voor reclamedoeleinden.[12] Hoewel de AVG en aanverwante wetgeving een sterk kader bieden voor de bescherming van persoonsgegevens blijven er uitdagingen. Om effectief toezicht te houden op internationale bedrijven en gegevensstromen is daarom blijvende inzet van het kabinet op internationale samenwerking nodig.

Tot slot kwam in het mondelinge vragenuur de vraag aan bod of de aanbieders op het platform van het Duitse bedrijf Datarade persoonsgegevens rechtmatig heeft verzameld en doorverkocht. De Minister voor Rechtsbescherming heeft met de Duitse Staatssecretaris van Justitie gesproken over de verkoop van persoonsgegevens met locatiegegevens via het Duitse platform. De Duitse Staatssecretaris van Justitie vertelde daarbij zeer alert te zijn op verschillende vormen van informatie-incidenten en is graag bereid hierover verder met Nederland van gedachten te wisselen. Het gesprek tussen Nederland en Duitsland over de algemene aanpak en deze specifieke casus in het bijzonder wordt op ambtelijk niveau voortgezet.

Toezicht en handhaving

Het toezicht op de toepasselijke wet- en regelgeving is een cruciaal onderdeel van de aanpak van privacy en gegevensbeschermingsvragen bij online handel in persoonsgegevens. In Nederland is de AP, die onafhankelijk opereert, belast met het toezicht op de naleving van de AVG. Het is aan de toezichthouder om per geval te beoordelen of wordt voldaan aan de eisen in de (U)AVG, en zo niet, of en op welke manier daartegen wordt opgetreden. De AP werkt daarbij met het oog op een consistente toepassing van de AVG bij grensoverschrijdende gegevensverwerkingen, samen met toezichthouders in andere lidstaten. Daarbij heeft de AP om uitvoering te kunnen geven aan zijn onderzoekstaak diverse onderzoeks- en handhavingsbevoegdheden. Zo kan de AP onderzoek instellen naar de naleving van de gegevensbeschermingswetgeving en in het kader daarvan audits uitvoeren en gegevensverwerkingen inzien. Wanneer de AP een overtreding constateert, kan de AP een boete of dwangsom opleggen en bevelen tot het stopzetten van de gegevensverwerkingen.

Daarnaast is de Autoriteit Consument en Markt (ACM) verantwoordelijk voor het toezicht op artikel 11.7a van de Telecommunicatiewet, waar cookies en andere vormen van tracking onder vallen. De AP en ACM hebben een samenwerkingsprotocol om hierop samen te werken.

Zoals de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties in de Kamerbrief over Toezicht en handhaving cookies van 18 september 2023 aankondigde, heeft de AP structureel extra middelen van dit kabinet

[11] Plenaire verslagen | Tweede Kamer der Staten-Generaal
[12] HvJ EU 19 april 2024, C-604/22, ECLI:EU:C:2024:214 (IAB Europe).

gekregen om het toezicht op het gebruik van cookies te versterken.[13] In de startfase van 2024 tot en met 2026 krijgt de AP € 500.000 per jaar extra voor toezicht en handhaving op cookies en vanaf 2027 krijgt de AP hiervoor structureel € 350.000 per jaar erbij. Hierdoor kunnen burgers makkelijker aangeven dat ze hun gegevens niet willen delen voor online doorverkoop. De AP zet in op het snel boeken van de eerste resultaten, om zo de privacy van burgers beter te beschermen. In de startfase wil de AP zich richten op het publiceren van richtlijnen en *best practices* voor het gebruik van cookiebanners. Daarnaast zal de AP onderzoeken naar websites uitvoeren en, waar nodig, handhavend optreden door het opleggen van een last onder dwangsom, een verwerkingsverbod of een boete. Het kabinet wil dat burgers hierdoor meer regie krijgen over hun persoonsgegevens. Als eerste actie heeft de AP uitleg geboden over hoe organisaties cookiebanners moeten inrichten om op een goede manier toestemming te vragen.[14] Deze acties wil de AP vanaf 2027 voortzetten en waar nodig bijsturen.

Zoals aangekondigd in de Kamerbrief cookies en online tracking[15] wordt onder de verantwoordelijkheid van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aanvullend onderzoek gedaan naar alle vormen van tracking op overheidswebsites, met als doel deze te verminderen en alternatieven te bieden waarbij geen gegevens van burgers met derden worden gedeeld wanneer zij communiceren met de overheid.

In lijn met de Werkagenda Waardengedreven Digitaliseren, heeft het kabinet zich ingezet voor de verbetering van onze digitale dienstverlening en online transparantie voor burgers.

Bewustwording en verantwoordelijkheid

Het kabinet benadrukt het belang van bewustwording bij burgers en overheidsmedewerkers over de risico's verbonden aan gegevensverzameling in het digitale domein.

Dit omvat ook de verantwoordelijkheid van ambtenaren bij het gebruik van mobiele apparaten en mobiele applicaties. Overheidsmedewerkers met bepaalde risicoprofielen krijgen dan ook veiligheidsinstructies over waar ze rekening mee moeten houden in hun onlinegedrag. In maart 2023 heeft het kabinet aangegeven dat Rijksambtenaren zonder voorafgaande toestemming geen gebruik meer mogen maken van apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland.[16] Dit zijn landen zoals China, Rusland, Iran en Noord-Korea.[17] In de Kamerbrief Stand van zaken appbeleid van 24 november 2023 is uiteengezet welke stappen sinds de oorspronkelijke Kamerbrief uit maart zijn genomen.[18] Momenteel wordt door CIO-Rijk gewerkt aan een plan van aanpak voor het ontwikkelen en implementeren van zogeheten beheerde apparaten. Dit laat onverlet dat het gebruik van privéapparaten nog steeds kan leiden tot het vormen van risicovolle patronen op basis van verzamelde data op die apparaten.

De zorgen omtrent de online advertentie-industrie en de impact ervan op de nationale veiligheid nemen wij serieus. Zoals uiteengezet in deze brief zijn we actief bezig met het adresseren van deze problematiek. Het is

---

[13] Kamerstukken II 2023/24, 26 643, nr. 1071.
[14] AP pakt misleidende cookiebanners aan | Autoriteit Persoonsgegevens.
[15] *Kamerstukken II* 2022–2023, 32 761, nr. 286
[16] Kamerstukken II, 2022/23, 26 643, nr. 984
[17] Jaarverslagen | AIVD
[18] Kamerstukken II 2022/23, 26 643, nr. 1087.

duidelijk dat de uitdagingen complex zijn en een gecoördineerde aanpak vereisen. Wij blijven ons inzetten voor een veilige, transparante en waarde gedreven digitale omgeving, waarbij privacy en veiligheid voorop staan.

Hieronder volgt de reactie van het kabinet over de nationale veiligheid in relatie tot online-gegevensverzameling en wat het kabinet doet om dit te adresseren.

2. Poteniele risico van grootschalige gegevensverzameling voor de nationale veiligheid

In november 2022 is het «Dreigingsbeeld Statelijke Actoren 2» gepubliceerd waarin de AIVD, MIVD en Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) hun bevindingen delen over de grootschalige verzameling van persoonsgegevens door statelijke actoren.[19] In het dreigingsbeeld wordt de zorg onderstreept over de wijze waarop deze actoren op grote schaal gegevens verzamelen. Dit doen zij zowel uit open bronnen (onder andere uit sociale media-profielen en openbare registers), als uit gesloten bronnen (bijvoorbeeld door het hacken van hotelketens, telecombedrijven of medische instellingen). Dergelijke grootschalige vergaring van persoonsgegevens is zorgelijk, ook op de lange termijn. Statelijke actoren gebruiken de verworven persoonsgegevens namelijk op verschillende manieren. Zo kunnen persoonsgegevens worden gebruikt voor gerichte beïnvloedingsdoeleinden om bijvoorbeeld tegenstanders van een regime in diskrediet te brengen, of sociale spanningen te vergroten door polarisatie aan te wakkeren. Ook kunnen grote hoeveelheden aan persoonsgegevens gebruikt worden om technologieën verder te ontwikkelen, waarmee bijvoorbeeld militaire slagkracht en spionagecapaciteiten vergroot kunnen worden. Om de dreiging vanuit statelijke actoren het hoofd te bieden bestaat sinds 2019 de aanpak statelijke dreigingen. Met de Kamerbrief Aanpak Statelijke Dreigingen van 28 november 2022 bent u reeds geïnformeerd over bestendiging en versterking van de maatregelen die het kabinet hier tegenoverstelt.[20] Daarnaast is het voorstelbaar dat niet-statelijke actoren via de digitale advertentiemarkt toegang hebben tot persoonsgegevens van te beveiligen personen. Daar waar nodig worden op basis van dreiging en risico's de benodigde beveiligingsmaatregelen getroffen.

3. Bevoegdheden van de inlichtingen- en veiligheidsdiensten voor «OSINT»-onderzoeken

De AIVD en de MIVD kunnen bij hun onderzoeken bevoegdheden inzetten die in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) zijn vastgelegd. Een van de algemene bevoegdheden in de Wiv 2017 is het verwerken van informatie uit open bronnen. De inzet van bevoegdheden is omkleed met diverse waarborgen voor zorgvuldige gegevensverwerking, waarop toezicht wordt gehouden door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

Over het onderzoeken van open bronnen heeft de CTIVD in 2022 het toezichtsrapport 74 over Automated Open Source Intelligence (AOSINT) gepubliceerd. Hierin zijn geen onrechtmatigheden vastgesteld. Het kabinet heeft de aanbevelingen van de CTIVD overgenomen.[21] Tevens hebben de AIVD en MIVD reeds een pilot afgerond ten behoeve van de inrichting van

[19] AIVD, MIVD en NCTV – Dreigingsbeeld Statelijke Actoren (2022).
[20] Kamerstukken II 2022–2023, 30 821, nr. 175
[21] Kamerstukken II 2021/22, 29 924, nr. 223

een afwegingskader rondom de inzet van AOSINT-tools. Hierover is uw Kamer in oktober 2023 geïnformeerd.[22]

Samenvattend is het kabinet zich volledig bewust van de risico's die de online advertentie-industrie vormt voor de privacy van burgers en de nationale veiligheid. In reactie hierop intensiveren we toezicht en handhaving, en vergroten wij het bewustzijn onder burgers over de verwerking van hun persoonsgegevens.

Met deze maatregelen tracht het kabinet de bescherming van persoonsgegevens effectief te verhogen en de veiligheid van de Nederlandse samenleving te waarborgen.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

De Minister voor Rechtsbescherming,
F.M. Weerwind

[22] Kamerstukken II 2023/24, 29 924, nr. 254