Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

32 761 Verwerking en bescherming persoonsgegevens

Nr. 174

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID EN VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 november 2020

Tijdens de Regeling van werkzaamheden op 16 oktober 2019 heeft het lid van uw Kamer Van Dam (CDA) om een standpunt gevraagd over de door hem waargenomen steeds vaker voorkomende strijd tussen privacybescherming en het opsporingsbelang.[1]

Nieuwe technologische ontwikkelingen raken ook de opsporing van strafbare feiten. De opsporingsdiensten moeten ook binnen een toenemend digitaliserende samenleving uit de voeten kunnen met de middelen die hen ten dienste staan. Kort gezegd is het zaak om binnen het spanningsveld tussen opsporing en privacy het evenwicht te blijven hanteren tussen slagvaardigde opsporing en eerbiediging van het grondrecht. In deze brief maken wij uw Kamer graag deelgenoot van onze inspanningen en visie op dit terrein.

Het recht op privacy: geen schild voor criminaliteit

Het recht op eerbiediging van de persoonlijke levenssfeer en het privéleven is een grondrecht dat verankerd is in verschillende verdragen, zoals het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM), het Handvest van de grondrechten van de Europese Unie, de Algemene verordening gegevensbescherming (AVG) en de EU-Richtlijn gegevensbescherming opsporing en vervolging[2]. Daarnaast vindt het recht op privacy bescherming in de Grondwet.

Het recht op privacy is niet absoluut. Artikel 8 van het EVRM bepaalt dat een staat dit recht mag beperken, als dat bij de wet is voorzien en in een democratische samenleving noodzakelijk is op grond van een aantal nader aangegeven gronden. Daartoe behoren onder meer het belang van de openbare veiligheid en het voorkomen van wanordelijkheden en het

[1] Handelingen 2019/20, nr. 14, item 8, p. 2.
[2] EU-richtlijn 2016/680.

kst-32761-174
ISSN 0921 - 7371
's-Gravenhage 2020

opsporen en vervolgen van strafbare feiten. Verder moet de beperking in alle gevallen voldoen aan de vereisten van proportionaliteit en subsidiariteit.
Dat impliceert dat de overheidshandeling waarmee de privacy wordt beperkt, evenredig moet zijn aan het belang dat ermee wordt gediend, en dat van de maatregel moet worden afgezien indien het doel dat daarmee wordt beoogd, ook langs een andere weg met minder ingrijpende middelen kan worden bereikt. Artikel 52 van het Handvest van de grondrechten van de Europese Unie kent een hiermee vergelijkbare beperkingsmogelijkheid en ook artikel 10 van de Grondwet biedt de mogelijkheid om het recht op privacy te beperken, mits die beperkingen bij of krachtens een wet in formele zin moeten zijn vastgelegd.

Privacy en opsporing

Een van de wetten die een grondslag biedt voor het maken van inbreuk op de privacy, is het Wetboek van Strafvordering (WvSv). Opsporingsbevoegdheden mogen op grond daarvan alleen worden ingezet op een wijze die bij de wet is voorzien, doch niet voor alle manieren van opsporing geldt een afzonderlijke wettelijke voorziening in het WvSv. Zo kan een wijze van opsporen die niet een meer dan beperkte inbreuk op de persoonlijke levenssfeer maakt, in beginsel zonder specifieke regeling plaatsvinden. De rechtsbasis kan in dat geval in algemene taakstellende bepalingen worden gevonden. Wanneer er een méér dan beperkte inbreuk op de privacy nodig is, dan dient daarvoor een specifiekere wettelijke grondslag te bestaan. Daarbij kan bijvoorbeeld worden gedacht aan de bepalingen met betrekking tot opsporingsbevoegdheden, zoals stelselmatige observatie, stelselmatige inwinning van informatie, het betreden van besloten plaatsen, het opnemen van vertrouwelijke communicatie, het onderzoeken van een computer en het vorderen van gegevens.

In de praktijk is echter gebleken dat het huidige WvSv onvoldoende aansluit bij de huidige digitale samenleving. Zo geeft de wet geen duidelijkheid over de situatie waarin na inbeslagneming van een smartphone nog berichten binnenkomen op dit apparaat, waardoor onduidelijk is of opsporingsinstanties deze berichten mogen lezen en gebruiken voor het opsporingsonderzoek. Bovendien bevat de wet thans geen specifieke regeling voor onderzoek in smartphones, terwijl deze in nagenoeg ieder opsporingsonderzoek een rol spelen. Het is (onder meer) in deze gevallen onduidelijk op welke wijze de afweging tussen de belangen van privacy en opsporing volgens de wetgever zou moeten worden gemaakt. Dit levert in de praktijk een spanningsveld op; er bestaat immers onzekerheid over de vraag of een opsporingsbevoegdheid mag worden ingezet. In sommige gevallen zal de opsporing de inzet van een opsporingsbevoegdheid achterwege laten, simpelweg omdat zij vreest dat deze achteraf door de rechter onrechtmatig zal worden bevonden en de strafzaak zal schaden.

De wettelijke regeling van het opsporingsonderzoek wordt, mede in het licht van de toenemende digitalisering, bij de voorgenomen modernisering van het WvSv vernieuwd. Daarbij wordt uitvoering gegeven aan diverse aanbevelingen van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (de commissie-Koops).[3] In het concept van het nieuwe Wetboek van Strafvordering is bij deze modernisering van de opsporingsbevoegdheden telkens een zorgvuldige afweging gemaakt over de wettelijke voorwaarden waaronder met deze bevoegdheden een inbreuk op de privacy mag worden gemaakt.

[3] Zie het rapport van de commissie «Regulering van opsporingsbevoegdheden in een digitale omgeving», d.d. 26 juni 2018.

Uw Kamer wordt separaat over de voortgang van het project tot modernisering van het Wetboek van Strafvordering op de hoogte gehouden.

Wettelijke opsporingsbevoegdheden staan zoals gezegd een inbreuk op de privacy toe. Dat neemt niet weg dat voorafgaand aan de uitoefening daarvan, altijd een afweging plaats te vinden of dat in een specifiek geval ook in overeenstemming is met de beginselen van proportionaliteit en subsidiariteit. Dit geldt voor elke betrokkene in de keten, van opsporingsambtenaar tot officier van justitie en rechter(-commissaris). Deze verplichte afweging dwingt bijvoorbeeld om van een opsporingsmethode af te zien als het relatief een te zwaar middel is ten opzichte van de ernst van het strafbaar feit dat moet worden opgespoord. In het geval een opsporingsmiddel wordt ingezet, dient altijd te worden bezien of een minder ingrijpend middel ook toereikend is en dient de inzet daarvan waar mogelijk te worden beperkt in tijd of intensiteit. Op deze wijze wordt ook bij de praktische uitvoering van opsporingsbevoegdheden het evenwicht tussen privacy en opsporing bewaard. De noodzaak daarvan wordt onderstreept doordat in het concept van het nieuwe Wetboek van Strafvordering de beginselen van proportionaliteit en subsidiariteit in algemene bepalingen van het opsporingsonderzoek zijn gecodificeerd.

Tred houden met actuele ontwikkelingen

In een samenleving die steeds verder digitaliseert, laat ook criminaliteit steeds meer digitale sporen na en vindt zij plaats in een omgeving die in toenemende mate andere relevante data voor de opsporing kan bevatten. Dat geldt niet alleen voor criminaliteit die gericht is op digitale systemen, zoals cybercrime, maar ook voor criminaliteit waarbij digitalisering hooguit een ondersteunende rol heeft, zoals online fraude en witwassen met de daarvoor gebruikte financiële transacties in digitale vorm. Daarbovenop geldt dit voor criminaliteit die in het fysieke domein plaatsvindt, zoals liquidaties en drugshandel, aangezien ook deze criminelen steeds meer gebruik maken van digitale communicatiemiddelen en opslag. Als gevolg van deze ontwikkeling zijn er steeds meer data die direct of indirect naar verdachten en uiteindelijk daders kunnen leiden.

Digitaal bewijs wordt aldus steeds belangrijker. Vanwege het internationale karakter van het internet en dataopslag «in de cloud» is het grensoverschrijdend vorderen van elektronisch bewijs steeds belangrijker. Hiervoor bestaan diverse initiatieven in de EU (E-evidence) en de Raad van Europa (Tweede aanvullend protocol bij het cybercrimeverdrag).

Waar informatie in nieuwe toepassingen moeilijker bereikbaar wordt voor de opsporing, wordt een vertaalslag gevergd om bevoegdheden die van oudsher zien op «analoge» situaties ook in het digitale domein toe te passen. Denk aan de ontwikkeling van het 5G-netwerk, toenemende toepassing van anonimiserende technologie zoals encryptie (waardoor tappen in de traditionele zin moeilijker is) en de toegenomen beveiliging op smartphones. Om opsporingsbevoegdheden en -middelen effectief en bij de tijd te laten blijven, wordt op dit moment bezien wat de mogelijkheden zijn rond rechtmatige toegang tot versleutelde communicatie en de voor- en nadelen daarvan.[4]

De grotere hoeveelheid informatie, toenemende rekenkracht en betere databewerkingtechnieken waardoor steeds meer kennis uit data kan worden gehaald, zorgen voor toenemende mogelijkheden voor door data gedreven opsporing. De opsporing krijgt door het gebruik van moderne

[4] Kamerstuk 26 643, nr. 383.

analysetechnieken steeds meer zicht op criminele activiteiten, terwijl er nog geen concrete verdachte is. Fenomenen worden bestudeerd van waaruit verdenkingen kunnen ontstaan. Met behulp hiervan is het mogelijk om op basis van data patronen te ontdekken die op criminaliteit kunnen wijzen. Het kan hier gaan om zowel opsporingsinformatie die al beschikbaar is, als informatie van andere organisaties, waarmee men gezamenlijk gegevens verwerkt in samenwerkingsverbanden. Ook worden in toenemende mate instrumenten gebruikt om risicotaxaties uit te voeren die verdachte gedragingen in het vizier kunnen brengen. Dit kan sturingsinformatie opleveren die de inzet van recherchecapaciteit effectiever en efficiënter maakt.

In dit kader van de te betrachten zorgvuldigheid speelt het Kwaliteitskader Big Data[5], dat is opgesteld door de politie en het OM, een belangrijke rol. Dit wordt gebruikt voor het toetsen van big data toepassingen aan rechtmatigheid en ethiek. Hierin komen onder meer terug de richtlijnen voor het toepassen van algoritmes door de overheid uit de brief van 8 oktober 2019[6]. Het kwaliteitskader ziet op de ontwikkeling en toepassing van algoritmes en data-analysemethoden in de opsporing.

Moderne analysetechnieken winnen ten slotte niet alleen aan betekenis wanneer er nog geen verdachte in beeld is, zij spelen ook een belangrijke rol in de fase dat er al een verdenking bestaat en data strafvorderlijk is vergaard of verstrekt op vordering van de officier van justitie of rechtercommissaris. Zo is het steeds beter mogelijk om met nieuwe technieken enorme hoeveelheden telecommunicatie te verwerken, zoals onlangs nog is gebleken bij berichten van klanten van EncroChat uit de kring van de onderwereld, waarbij uit de grote hoeveelheid berichten bijvoorbeeld indicaties voor corruptie onder politiemedewerkers konden worden gehaald.

Verdere versterkingen van de opsporing

Hoge prioriteit heeft voor ons de bestrijding van georganiseerde, ondermijnende criminaliteit, waarvoor privacy geen schild mag vormen. Deze vorm van criminaliteit tast de wortels van onze rechtsstaat aan en vraagt daarom om extra inspanningen om die te bestrijden. De gevaren voor de lokale samenleving zijn immers evident: drugslabs, schietpartijen en liquidaties in woonwijken en de openbare ruimte, exorbitante criminele winsten, parallelle samenlevingen, intimidatie en corruptie.[7]

Een van die maatregelen is de oprichting van het Multidisciplinair Interventieteam (MIT), waarbinnen zeven organisaties samenwerken met als doelstelling om vanuit een data-gedreven aanpak kwetsbaarheden in – op zichzelf beschouwd – rechtmatige structuren in beeld te krijgen. Hierdoor kan beter inzichtelijk worden gemaakt hoe criminele netwerken er uit zien, hoe criminele processen werken en hoe fenomenen in elkaar steken (financieel, logistiek, relationeel, bedrijfsstructuur etc.). In onderlinge afstemming zet iedere partner binnen het MIT op grond van zijn eigen taak en verantwoordelijkheid zijn eigen bevoegdheden in. Het gaat dan om zowel financiële opsporing (straf- en fiscaalrechtelijk) als toezicht en handhaving (fiscaal-, civiel- en bestuursrechtelijk).
Op de gegevensdeling binnen het MIT zijn de wettelijke kaders van toepassing die gelden voor de individuele deelnemers, zoals de Wet politiegegevens. Om inbreuken op de privacy te mitigeren en om recht te

[5] https://www.rijksoverheid.nl/documenten/rapporten/2020/05/29/tk-bijlage-2-kwaliteitskader-big-datas.
[6] Kamerstuk 29 628, nr. 641.
[7] Kamerstuk 29 911, nr. 281, p. 4.

doen aan de principes van proportionaliteit en subsidiariteit, onderzoekt een werkgroep informatiedeling onder leiding van ons ministerie welke mogelijkheden de betrokken organisaties in het MIT op dit moment hebben om informatie te delen en op welke wijze de gewenste informatiedeling mogelijk kan worden gemaakt.[8]

Versterking van de juridische basis onder de uitwisseling van informatie en het gezamenlijk verwerken daarvan, staat ook centraal in het wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS, Kamerstuk 35 447). Dat wetsvoorstel strekt er onder andere toe om voor samenwerkingsverbanden als de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), het Financieel Expertise Centrum en de RIEC's voorwaarden vast te leggen waaronder de deelnemers gezamenlijk data-analyses kunnen uitvoeren, en om te komen tot oplossingen in huidige sectorale bepalingen op het gebied van informatie-uitwisseling.[9] Het is mogelijk om op termijn bij algemene maatregel van bestuur nieuwe samenwerkingsverbanden onder de wet te laten vallen. In de WGS zijn tal van waarborgen opgenomen om een zorgvuldige verwerking van persoonsgegevens te bevorderen die recht doet aan de principes van het gegevensbeschermingsrecht. De nota naar aanleiding van het verslag inzake dit wetsvoorstel (Kamerstuk 35 447, nr. 6) en een nota van wijziging (Kamerstuk 35 447, nr. 7) zijn op 16 oktober jl. naar uw Kamer gestuurd.

Slot

In deze brief hebben wij geschetst hoe de opsporing voortdurend inspeelt op nieuwe technologieën. Het is inherent aan opsporing dat inbreuk wordt gemaakt op de privacy. Kern van opsporing is immers het verzamelen van informatie, waaronder persoonsgegevens. Daarbij moet voor ogen worden gehouden dat een inbreuk op de privacy van een verdachte of van derden (verdere) schendingen van grondrechten van slachtoffers door criminelen kan helpen voorkomen. Een rechtmatige toepassing van de wettelijke bevoegdheden levert geen schending van dat grondrecht op. Er is dan immers voldaan aan de voorwaarden die aan een inbreuk gesteld worden.

Het nieuwe Wetboek van Strafvordering zal bijdragen aan het verminderen van het spanningsveld tussen privacybescherming en opsporing, omdat dan ook bij de toepassing van digitale opsporingsmethoden duidelijk uit de wet volgt onder welke voorwaarden die een (meer dan beperkte) inbreuk mogen maken op de privacy.

Wij hechten eraan om, uiteraard met inachtneming van de voorwaarden, de opsporingsdiensten en het Openbaar Ministerie gelijke tred kunnen blijven houden met ontwikkelingen in het criminele milieu.
Het gebruik van nieuwe ontsleutelingstechnieken om geavanceerde encryptietechnieken bij te benen, is daar een treffend voorbeeld van.

Wij vertrouwen erop dat met deze brief is voldaan aan de wens van uw Kamer om meer inzicht te krijgen in het spanningsveld tussen privacybescherming en het opsporingsbelang.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Minister voor Rechtsbescherming,
S. Dekker

---

[8] Kamerstuk 29 911, nr. 281, p. 6.
[9] Kamerstuk 35 447, nrs. 1–3.