Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

643

Vragen van leden **Kathmann** en **Mutluer** (beiden GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid en de Minister en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de uitspraak van het Europese Hof van Justitie over het uitlezen van mobiele telefoons* (ingezonden 8 oktober 2024)

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 25 november 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 417.

Vraag 1
Bent u bekend met de uitspraak van het Europese Hof van Justitie van 4 oktober 2024, waarin wordt gesteld dat nationale wetgeving mag bepalen dat ook kleine misdrijven kunnen leiden tot het doorzoeken van telefoons?[1]

Antwoord 1
Ja.

Vraag 2
Wat is uw reactie op deze uitspraak van het Europese Hof? Wat is de reactie van de Nationale Politie? Kunt u ook de Autoriteit Persoonsgegevens vragen om haar zienswijze en deze doen toekomen aan de Kamer?

Antwoord 2
De rechtspraktijk in Nederland zal moeten uitwijzen wat de precieze betekenis van deze uitspraak is. Met de toepassing van de prejudiciële procedure wordt het Europese Hof van Justitie in toenemende mate om uitleg gevraagd van het EU-recht op het gebied van bevoegdheden in het kader van het strafrechtelijk onderzoek. De uitspraak in de zaak Bezirkshauptmannschaft Landeck past in deze ontwikkeling. De betekenis en de reikwijdte van deze rechtspraak voor de rechtspraktijk zijn nog onzeker. Zoals aangekondigd in de memorie van toelichting bij het wetsvoorstel tot vaststelling van een nieuw Wetboek van Strafvordering, wordt van de zijde van de regering een voorstel gedaan, zodra de betekenis en de reikwijdte van de rechtspraak van het Europese Hof

[1] Court of Justice of the European Union, 4 oktober 2024, Access by the police to data contained in a mobile telephone is not necessarily limited to the fight against serious crime (curia.Europa.eu/jcms/upload/docs/application/pdf/2024–10/cp240171en.pdf).

ah-tk-20242025-643
ISSN 0921 - 7398
's-Gravenhage 2024

van Justitie daarvoor voldoende zijn uitgekristalliseerd om deze in samenhang te kunnen codificeren[2]. Dan zal zoals gebruikelijk een wetsvoorstel in dit verband ter consultatie worden voorgelegd aan (onder meer) de politie en de Autoriteit persoonsgegevens. Dergelijke consultatieadviezen worden meegezonden aan uw Kamer bij de indiening van een wetsvoorstel.

Vraag 3
Bent u het met de indiener(s) eens dat men uiterst terughoudend moet zijn om het uitlezen van telefoons makkelijker te maken? Vindt u ook dat deze bevoegdheid enkel ingezet moet worden met toestemming van de rechter bij zware misdrijven?

Antwoord 3
Het Europese Hof van Justitie heeft bepaald dat de mogelijkheid om toegang te krijgen tot gegevens in een mobiele telefoon niet is beperkt tot strafrechtelijk onderzoek naar zware misdrijven, omdat anders een risico op straffeloosheid bij niet-zware misdrijven zou ontstaan en het doel van het in stand houden van een ruimte van vrijheid, veiligheid en rechtvaardigheid binnen de EU kan worden ondermijnd[3]. De ernst van het feit speelt volgens het Europese Hof van Justitie wel een belangrijke rol in de afweging die moet worden gemaakt. De betekenis van deze uitspraak voor de Nederlandse rechtsorde zal gaan blijken uit de rechtspraak in concrete gevallen.

Vraag 4
Wat is het huidige protocol voor het uitlezen van telefoons van verdachten? Wanneer wordt hier wel/niet toe besloten en welke toestemming is vereist voordat dit gebeurt? Is het protocol hetzelfde bij privételefoons als bij tweede telefoons die vermoedelijk gebruikt worden voor criminele activiteiten?

Antwoord 4
De voorwaarden voor toegang tot gegevens in een mobiele telefoon ten behoeve van de opsporing van strafbare feiten zijn vastgelegd in het Wetboek van Strafvordering, en verder ontwikkeld in het smartphonearrest van de Hoge Raad[4]. Oorspronkelijk is de toegang gestoeld op de bevoegdheid tot inbeslagneming van voorwerpen. De inbeslagnemingsbevoegdheid impliceert dat het inbeslaggenomen voorwerp kan worden onderzocht. De mobiele telefoon heeft zich als voorwerp echter zo ontwikkeld dat zeer veel (gevoelige) gegevens over de gebruiker of derden daarop kunnen worden opgeslagen, met als gevolg dat de toegang tot gegevens op een mobiele telefoon (zeer) ingrijpend kan zijn. Dit is voor de Hoge Raad aanleiding geweest tot het wijzen van het eerdergenoemde smartphonearrest. In dat arrest zijn voorwaarden gesteld wegens de mate van inbreuk op de persoonlijke levenssfeer die de toegang tot gegevens in een mobiele telefoon kan hebben. De algemene beginselen van proportionaliteit en subsidiariteit zijn bovendien van toepassing. Daarbij worden alle relevante feiten en omstandigheden gewogen, waaronder of er sprake is van een privé mobiele telefoon of een tweede mobiele telefoon die vermoedelijk gebruikt wordt voor criminele activiteiten. De rechtspraktijk zal gaan uitwijzen in hoeverre de toegang tot mobiele telefoons anders gaat verlopen dan voorheen door deze uitspraak van het Europese Hof van Justitie.

Vraag 5
Ziet u aanleiding om de bevoegdheid in nationale regelgeving verder uit te breiden tot lichte misdrijven? Zo ja, waaruit blijkt de noodzaak hiertoe? Hoe zwaar moet een misdrijf zijn voordat hiertoe volgens u besloten mag worden?

---

[2] Kamerstukken II 2022/23, 36 327, nr. 3, p. 334–335
[3] Overweging 97.
[4] ECLI:NL:HR:2017:584

Antwoord 5
Het EU-recht noch het nationaal recht vereist een verdenking van een zwaar misdrijf voor de toegang tot gegevens in een mobiele telefoon. Wel geldt dat de ernst van het strafbaar feit een belangrijke factor is bij de beoordeling van de toegang in een concreet geval.

Vraag 6
Hoe worden de belangen van opsporing, privacy, onschuldpresumptie en cyberveiligheid tegen elkaar afgewogen bij het besluit om wel of niet een telefoon uit te lezen?

Antwoord 6
Zie het antwoord op vraag 4.

Vraag 7
Hoe gaat het uitlezen van telefoons momenteel in werking, als de politie hiertoe besluit? Op welke manier wordt toegang verkregen tot een toestel? Wordt er wel eens gebruik gemaakt van biometrische gegevens van verdachten, zoals vingerafdrukken voor vingerafdrukscanners of gezichten (FaceID), om bij weigering van verdachten om een telefoon te ontgrendelen dit alsnog voor elkaar te krijgen en zo ja, hoe vaak komt dat voor? Wordt de data op een telefoon gericht uitgelezen op basis van het strafbare feit of wordt de hele telefoon – inclusief privécommunicatie – doorzocht? Worden de gegevens gekopieerd en opgeslagen, en zo ja, met welke bewaartermijn?

Antwoord 7
De politie sluit de telefoon over het algemeen aan op uitleesapparatuur en maakt een forensische kopie van bepaalde bestanden op het toestel of een exacte kopie van alle computergegevens, afhankelijk van de inhoud van het bevel. Soms wordt de mobiele telefoon handmatig onderzocht. Het komt voor dat een mobiele telefoon alleen ontgrendeld kan worden met behulp van biometrische gegevens van de gebruiker van dat toestel. De politie mag in die gevallen de verdachte vragen zijn toestel te ontgrendelen. Als de verdachte hier niet aan wil meewerken, mag de politie dwang gebruiken. Dit is bekrachtigd door de Hoge Raad in een arrest uit 2021[5]. Deze bevoegdheid is via de Innovatiewet Strafvordering vooralsnog opgenomen in artikel 558 van het Wetboek van Strafvordering. De rapporten waarin verslag is gedaan van de evaluatie van de Innovatiewet Strafvordering zijn onlangs verzonden aan uw Kamer[6]. Volgens de onderzoekers wordt de bevoegdheid regelmatig toegepast. Exacte cijfers zijn niet beschikbaar. Voor het einde van het jaar ontvangt uw Kamer de beleidsreactie op de evaluatierapporten.
De gegevens die zijn overgenomen worden door de politie opgeslagen, waarna (een deel van) deze gegevens toegankelijk worden voor gebruik door daartoe geautoriseerde opsporingsambtenaren die belast zijn met de opsporing van het strafbare feit waarvoor de mobiele telefoon in beslag is genomen. Deze gegevens vallen onder het regime artikel 9 in de Wet politiegegevens (Wpg). Deze gegevens kunnen worden gebruikt voor het opsporingsonderzoek en het eventueel daarop volgende strafproces, totdat een onherroepelijke beslissing in de betreffende zaak is genomen of de straf/maatregel volledig ten uitvoer is gelegd. Uiterlijk een half jaar nadat het doel van het onderzoek is bereikt, moeten de gegevens worden verwijderd. De systematiek in de Wpg schermt verwijderde gegevens af van andere gegevens en deze worden gedurende een periode van vijf jaar bewaard. Gedurende deze periode zijn de gegevens alleen toegankelijk voor een beperkt aantal poortwachters en kunnen slechts gebruikt worden voor enkele genoemde doelen. Na ommekomst van deze termijn moeten gegevens worden vernietigd.

Vraag 8
Kunt u deze vragen afzonderlijk van elkaar en zo spoedig mogelijk beantwoorden?

---

[5] ECLI:NL:HR:2021:202
[6] Kamerstukken II, 2024–2025, 35 869, nr. 31.

Antwoord 8
Ja.