

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over het ontwerpbesluit houdende vaststelling van het Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk) (Kamerstuk 34 372, nr. 28).

INHOUDSOPGAVE	blz.
I. Vragen en opmerkingen vanuit de fracties	1
1. Algemeen	1
2. Inleiding	2
3. Het onderzoek in een geautomatiseerd werk	2
3.1 Deskundigheid van opsporingsambtenaren	2
3.2 De uitvoering van een bevel van de officier van justitie	3
3.3 De vastlegging van gegevens over de uitvoering van een bevel in logbestanden	3
3.4 Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen	3
3.5 Het verrichten van onderzoekshandelingen in een geautomatiseerd werk	4
3.6 Verstrekking van ter uitvoering van een bevel vastgelegde gegevens	4
4. Gegevensverwerking	4
5. Toezicht	5
6. De toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens	5
7. Overig	5
II. Reactie van de Minister van Justitie en Veiligheid	5

I. Vragen en opmerkingen vanuit de fracties

1. Algemeen

De leden van de CDA-fractie hebben met interesse kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. Het stemt deze leden positief dat er in het besluit uitvoerig en gedegen uiteen is gezet hoe de procedure voor het doen van een onderzoek in een geautomatiseerd werk is vormgegeven. Bij een dergelijke zware bevoegdheid is van belang dat de procedures met waarborgen zijn omkleed en dat deze procedures goed worden nageleefd. Voornoemde leden zien dit terugkomen in het besluit, maar hebben nog wel enkele vragen.

De leden van de D66-fractie hebben kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. De leden zijn content met het feit dat de regering er bij de uitvoering van de Wet computercriminaliteit III (Kamerstuk 34 372) voor zorgt dat de markt in onbekende kwetsbaarheid zo min mogelijk wordt gestimuleerd en de schade aan cyberveiligheid zo klein mogelijk is. Slechts in een specifieke zaak, en als minder schadelijke alternatieven (gebruik van inloggegevens, social engineering of bekende

kwetsbaarheden) zijn doorlopen, mag hacksoftware worden ingekocht. Leveranciers van dergelijke software worden gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en verkopen niet aan dubieuze regimes. Bovendien worden statistieken over het gebruik van hacksoftware jaarlijks openbaar gemaakt. Deze leden zien dit als een significante verbetering ten opzichte van de bestaande situatie waarin opsporingsdiensten onbeperkt hacksoftware konden inkopen en daarmee de markt in onbekende kwetsbaarheden zouden stimuleren. Toch hebben voornoemde leden nog enkele vragen en opmerkingen.

De leden van de SP-fractie hebben met interesse kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. Zij hebben daarover nog wel enkele vragen.

2. Inleiding

De leden van de SP-fractie hebben de Wet computercriminaliteit III steeds zeer kritisch bekeken. Ook het Ontwerpbesluit onderzoek in een geautomatiseerd werk (Kamerstuk 34 372, nr. 26), dat de feitelijke uitwerking van de wet behelst, kon op de nodige kritische kanttekeningen rekenen van de genoemde leden en ook van de leden van D66-fractie. Zo vroegen de leden van de SP-fractie of hackbevoegdheden niet te veel uitgebreid zouden worden, en spraken zij hun zorgen uit over het gebruik van kwetsbaarheden in geautomatiseerde werken die door de opsporingsdiensten gebruikt kunnen worden (Kamerstuk 34 372, nr. 27, blz. 2 en 3). De leden van de SP-fractie vragen of het klopt dat het nu voorliggende besluit niet afwijkt ten opzichte van het ontwerpbesluit. Kan uiteen worden gezet op welke punten dit besluit toch afwijkt van het ontwerpbesluit en ook waarom? Wat is er nu precies met de stevige eerdere kritiek gedaan?

3. Het onderzoek in een geautomatiseerd werk

3.1 Deskundigheid van opsporingsambtenaren

De leden van de CDA-fractie lezen dat op grond van het Besluit onderzoek in een geautomatiseerd werk de genoemde ambtenaren worden aangewezen voor het onderzoek in een geautomatiseerd werk, indien zij lid zijn van een technisch team. Kunt u aangeven aan welke buitengewone opsporingsambtenaren als bedoeld in artikel 141 sub b, c en d, en artikel 142 van het Wetboek van Strafvordering moet worden gedacht? In welke gevallen zijn deze buitengewone opsporingsambtenaren lid van een technisch team?

Verder lezen voornoemde leden in het besluit dat de technische teams, in ieder geval gedurende de beginfase, centraal worden belegd in de politieorganisatie. Deze leden achten dit verstandig, maar vragen hoe het toezicht verloopt ten aanzien van de personen die geen lid zijn van een technisch team, maar wel worden aangewezen voor het doen van onderzoek in een geautomatiseerd werk? Verder vragen deze leden de regering of het is uitgesloten dat iemand van het tactisch team gevraagd kan worden eenmalig dan wel incidenteel onderzoek te doen in een geautomatiseerd werk?

De leden van de D66-fractie vragen een nadere toelichting op de opleidingseisen van opsporingsambtenaren. Wat voor soort kennis en vaardigheden moeten opsporingsambtenaren precies hebben om in aanmerking te komen voor deze functie? Is besef van dilemma's op het gebied van cybersecurity, zoals het stimuleren van de markt in «0-days» en ethiek, onderdeel van die opleidingseisen?

3.2 De uitvoering van een bevel van de officier van justitie

De leden van de CDA-fractie lezen dat uitvoering is gegeven aan de gemaakte afspraken in het Regeerakkoord 2017–2021 ten aanzien van de hacksoftware. Kunt u aangeven of de extra te maken kosten van de hacksoftware opgevangen worden door de in het Regeerakkoord toegezegde gelden voor de uitvoering van de Wet Computercriminaliteit III? Kunt u bevestigen dat de kosten van een technisch hulpmiddel of van een onderzoek niet doorslaggevend zullen zijn in de afweging of een bevoegdheid zal worden ingezet?

Ten aanzien van de ambtenaren die door de korpschef zijn aangewezen om als enige toegang te hebben tot de vastgelegde gegevens die zijn verzameld bij het verrichten van onderzoekshandelingen, vragen voornoemde leden of deze ambtenaren ook onderdeel (kunnen) zijn van het technische team.

De leden van de D66-fractie constateren dat alleen in uiterste gevallen gebruik gemaakt mag worden van commerciële hacksoftware. Daarbij stelt u dat deze software alleen kan worden gebruikt wanneer minder ingrijpende middelen zoals het gebruik van inloggegevens, social engineering of bekende kwetsbaarheden niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk. Op welke manier wordt vastgesteld dat deze minder ingrijpende en minder schadelijke middelen niet toereikend zijn? Deelt u de mening dat de ontoereikendheid van een techniek als social engineering alleen geconstateerd kan worden door het toepassen van de techniek op de betreffende verdachte? Kan een rapport haalbaarheidsonderzoek het voorstel voor het inkopen van commerciële hacksoftware bevatten als niet eerst minder ingrijpende en minder schadelijke alternatieven zijn geprobeerd? Welke eisen worden gesteld aan de beveiliging van de technische infrastructuur waarop gegevens tijdens het verrichten van onderzoeksafdelingen worden geregistreerd? Bent u bereid bij het publiceren van statistieken over het gebruik van software te specificeren in hoeveel zaken commerciële hacksoftware is ingekocht?

3.3 De vastlegging van gegevens over de uitvoering van een bevel in logbestanden

De leden van de D66-fractie vragen een nadere toelichting op het procedureel vastleggen binnen de politieorganisatie dat handmatige logging plaatsvindt. Wat wordt er verstaan onder handmatige logging? In hoeverre is dit, gezien het belang van de betrouwbaarheid en integriteit van vastgelegde gegevens, wenselijk? Welke eisen worden gesteld aan de technische infrastructuur waarop de logging-gegevens worden opgeslagen? Bevinden deze technische infrastructuur of servers zich altijd in Nederland?

3.4 Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

De leden van de CDA-fractie lezen dat de Dienst landelijke operationele samenwerking belast wordt met de keuring van technische hulpmiddelen die gebruikt worden voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Op dit moment is deze dienst belast met de traditionele technische hulpmiddelen die worden ingezet bij stelselmatige observatie, zo begrijpen deze leden. Hoe schat u het kennisniveau van deze dienst in het terrein van technische hulpmiddelen die het mogelijk maken geautomatiseerde werken binnen te dringen? Deze leden vermoeden dat in sommige gevallen complexe technische hulpmiddelen ingezet en gekeurd moeten gaan worden en achten het van belang dat dit

goed gebeurt. Welke ondersteuning ten aanzien van verbetering van het kennisniveau op dit moment en in de toekomst kan de Dienst verwachten? Ook vragen voornoemde leden hoe er is nagedacht over de toepassing van software die gebruikt maakt van algoritmes en wellicht in de toekomstig kunstmatige intelligentie. Hoe wordt er bijvoorbeeld op toegezien dat de werking van deze algoritmes altijd uitlegbaar blijft zodat het technisch gekeurd kan worden? Wordt er in dergelijke gevallen rekening gehouden met de omstandigheid dat het uitlegbaar is voor de rechter die mogelijk bij de behandeling van de strafzaak de volledige informatie opvraagt over de verrichte onderzoekshandelingen?

De leden van de D66-fractie vragen u nader toe te lichten of de technische infrastructuur waarop onderzoeksgegevens worden opgeslagen altijd in beheer zijn van de politie. Kan het ook voorkomen dat de infrastructuur in beheer is van de verkoper van commerciële hacksoftware? Bevindt deze technische infrastructuur zich altijd in Nederland? Wat is de reden dat de wijze waarop het binnendringen bij het gebruik van commerciële hacksoftware plaatsvindt geen onderdeel uitmaakt van het keuringsproces? Is dat niet juist noodzakelijk bij het bepalen van de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden?

3.5 Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

De leden van de CDA-fractie lezen dat een technisch hulpmiddel dat niet van tevoren is gekeurd in bepaalde gevallen kan worden ingezet worden. Deze uitzondering geldt als het onderzoeksbelang dit dringend vordert en in dergelijke gevallen wordt het hulpmiddel achteraf gekeurd of, in uiterste gevallen, niet gekeurd. Deze leden vragen of bij de achteraf keuring van het hulpmiddel ook wordt bepaald of het middel op de juiste manier is ingezet. Wat gebeurt er in het geval het hulpmiddel wordt afgekeurd, maar al wel is ingezet bij onderzoekshandelingen? Welke gevolgen heeft dit voor het onderzoek?

3.6 Verstrekking van ter uitvoering van een bevel vastgelegde gegevens

De leden van de D66-fractie vragen een nadere toelichting op «bewerking» in het geval een selectie gemaakt moet worden van de vastgelegde gegevens. Welke procedurele waarborgen zijn mogelijk indien onderzoekshandelingen zonder technische hulpmiddel worden verricht? Klopt het dat het in dit geval concreet gaat om het gebruik van de verdachte buitgemaakte inloggegevens? Is er een standaard methode van logging in een dergelijke situatie?

4. Gegevensverwerking

De leden van de D66-fractie constateren dat gegevens die tijdens een onderzoek worden buitgemaakt tevens persoonsgegevens kunnen bevatten van onschuldige mensen die geen verdachte zijn. Hoe wordt de privacy van deze mensen geborgd en worden gegevens van deze mensen vernietigd? Kunt u de volgende zin nader toelichten: «De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd (artikel 14, eerste lid, Wet politiegegevens).»? Hoe kunnen «verwijderde gegevens» alsnog vijf jaar bewaard worden? Hoe kunnen «verwijderde gegevens» gearchiveerd worden?

5. Toezicht

De leden van de SP-fractie vinden dat het toezicht van de Inspectie Justitie en Veiligheid op de uitvoering van de in het wetsvoorstel opgenomen bevoegdheden kwalitatief goed moet zijn. Zijn inmiddels voldoende mensen met kennis en expertise in dienst bij de Inspectie om goed toezicht te kunnen houden? Zo ja, kan dit nader onderbouwd worden? Zo nee, waarom (nog) niet?

6. De toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

De leden van de D66-fractie vragen u nader in te gaan op het punt van de Nederlandse Orde van Advocaten dat de aanwijzing van het misdrijf «witwassen» surveillance toestaat van ieder persoon met niet onmiddellijk verklaarbaar bezit. Kunt u inhoudelijk reageren op dit bezwaar? Bent u bereid bij de evaluatie van de Wet computercriminaliteit III uiteen te zetten hoe vaak voor welk soort misdrijf de bevoegdheid is ingezet?

7. Overig

De leden van de SP-fractie zijn op de hoogte van het voornemen tot evaluatie van de Wet computercriminaliteit III. Kan een uitkomst van deze evaluatie te zijner tijd ook zijn dat de bevoegdheid om een geautomatiseerd werk binnen te dringen zou moeten gelden voor minder misdrijven dan nu in het besluit opgenomen? Zo nee, waarom niet?

II. Reactie van de Minister van Justitie en Veiligheid

De voorzitter van de commissie,
Van Meenen

De adjunct-griffier van de commissie,
Schoor