Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

29 924 Toezichtsverslagen AIVD en MIVD

Nr. 224 **BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 maart 2022

Hierbij bieden wij u rapport nr. 75 van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) aan[1]. Het rapport gaat over de snapshotfase bij de inzet van kabelinterceptie door de AIVD en de MIVD. De snapshotfase gaat vooraf aan de inzet van kabelinterceptie ten behoeve van de onderzoeksopdrachten (de zogenoemde productiefase). De CTIVD heeft zich in haar onderzoek gericht op de periode van 1 mei 2018 tot en met 31 maart 2021. Wij danken de CTIVD voor het gedegen onderzoek en het rapport, dat duidelijk beschrijft onder welke complexe omstandigheden de diensten hebben gewerkt om kabelinterceptie te operationaliseren. Het onderzoek van de CTIVD en dit rapport zijn voor de diensten zeer behulpzaam bij het inrichten en verantwoord kunnen blijven uitvoeren van kabelinterceptie. Wij onderschrijven daarom de conclusies van de CTIVD en nemen alle aanbevelingen over.

Algemeen

Kabelinterceptie is onderzoeksopdrachtgerichte interceptie (OOG-interceptie) op de kabel en betreft het in bulk onderscheppen van communicatie, hetgeen betekent dat er sprake is van een bepaalde mate van ongerichtheid bij het verzamelen van gegevens. De interceptie dient wel te relateren aan één of meerdere onderzoeksopdrachten van de diensten. Deze specifieke bijzondere bevoegdheid is geïntroduceerd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en is van essentieel belang om verborgen dreigingen in onder meer het cyberdomein te onderkennen. Dankzij de ervaringen en inzichten die zijn opgedaan kan nu veel beter dan vijf jaar geleden een duidelijk beeld worden gegeven van kabelinterceptie.

Het *snapshotten* is een voorwaarde om zo gericht mogelijk kabelinterceptie in te kunnen zetten en wordt in het rapport gedefinieerd als het

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-29924-224
ISSN 0921 - 7371
's-Gravenhage 2022

doen van korte integrale opnames van de beschikbare gegevensstromen om de veronderstelde inlichtingenwaarde te kunnen vaststellen. De onderzoeksperiode omspant de fase die loopt van het benaderen van een aanbieder van communicatiediensten tot en met het uitvoeren van deze snapshots. In deze fase is nog geen sprake van kabelinterceptie ten behoeve van het inlichtingenproces, omdat de gegevens die worden verkregen uit de snapshots niet mogen worden gebruikt voor inhoudelijk onderzoek. Deze opnames worden enkel onderzocht met het oog op het optimaliseren van de interceptie ten behoeve van het inlichtingenproces, oftewel productie.

Bevindingen en conclusies

De CTIVD concludeert dat de AIVD en de MIVD bij het realiseren van de accesslocatie (de locatie waar de interceptie van de datastroom fysiek plaatsvindt) op belangrijke onderdelen rechtmatig hebben gehandeld. Zo hebben de diensten met de informatieplicht alleen wettelijk toegestane informatie opgevraagd en was ten tijde van het technisch operationaliseren van de accesslocatie sprake van een geldige toestemming. De AIVD en de MIVD hebben bij het *snapshotten* invulling gegeven aan het gerichtheidscriterium. De diensten hebben de geïntercepteerde gegevens tijdig vernietigd en hebben deze niet gedeeld met buitenlandse diensten. De CTIVD concludeert voorts dat de diensten bij het *snapshotten* technisch en juridisch hebben moeten pionieren in een complexe omgeving en daardoor op onderdelen onrechtmatig hebben gehandeld. Door de complexiteit van dit proces zijn in het kader van de wettelijke zorgplicht aan sommige technische, personele en organisatorische maatregelen onvoldoende invulling gegeven, wat als gevolg heeft gehad dat er onrechtmatigheden in het interceptieproces zijn ontstaan. Zo concludeert de CTIVD dat bijzondere bevoegdheden ter ondersteuning van het operationaliseren van kabelinterceptie zonder toestemming zijn ingezet en werkzaamheden bij de communicatieaanbieder hebben plaatsgevonden na het aflopen van toestemmingstermijnen. Tevens zijn bepaalde waarborgen, zoals *logging* en controle, onvoldoende nageleefd, waardoor een zeer beperkt gedeelte van de gegevens voor een korte periode toegankelijk is geweest voor de inlichtingenteams.

Het intercepteren en het opslaan van communicatie brengt inherent een inbreuk mee op de fundamentele rechten van burgers. Ten aanzien van de mate van deze inbreuk concludeert de CTIVD dat in de onderzoeksperiode communicatie is geïntercepteerd en opgeslagen door de diensten, dat deze gegevens zijn doorzocht en onderzocht maar dat dit vrijwel uitsluitend is gebeurd vanuit een technisch perspectief, met als doel het beoordelen van de potentiele inlichtingenwaarde van de geïntercepteerde gegevens. De gegevens zijn niet gebruikt in inlichtingenproducten. Door de diensten zijn de bewaartermijnen nageleefd en zijn gegevens na een jaar vernietigd. Ten slotte zijn alleen kanalen geïntercepteerd waarvoor toestemming is verkregen en zijn geen gegevens gedeeld met buitenlandse inlichtingen en veiligheidsdiensten. Deze constatering leidt tot de conclusie dat sprake is van een inbreuk op fundamentele rechten van burgers, maar dat deze inbreuk beperkt is geweest.

Aanbevelingen

De CTIVD doet een drietal aanbevelingen, die wij overnemen en voor het overgrote deel reeds hebben uitgevoerd. De eerste aanbeveling, die inmiddels ook al is uitgevoerd, betreft het beleggen van de eindverantwoordelijkheid voor de gehele interceptieketen van verwerving en (verdere) verwerking op centraal en voldoende hoog niveau, zodat sprake is van doorzettingsmacht binnen beide organisaties. De tweede

aanbeveling ziet op de invulling van de wettelijke zorgplicht door onder andere instrumenten in te richten ten behoeve van interne controle en effectief extern toezicht, waaronder de beschikbaarheid van *logging* voor compliance-monitoring en bestaande beleid en werkinstructies af te stemmen op ontstane praktijk van het *snapshotten*. Tot slot ziet de derde aanbeveling op vastlegging in werkinstructies en beleid van toestemmingstermijnen, wijze van inzet en reikwijdte van de informatieplicht en de medewerkingsplicht. De diensten zijn, in overleg met de CTIVD, bezig met de uitvoering van de tweede en de derde aanbeveling.

De AIVD en MIVD zijn reeds gedurende het onderzoek gestart met de verbetermaatregelen, waaronder de uitvoering van een reeds opgesteld verbeterplan. Dit verbeterplan, dat ook deels op aanbeveling 2 ziet, dient ter versterking van de interne controle op gegevensverwerving en gegevensverwerking van beide diensten. Het plan is begin november 2021 met de CTIVD gedeeld. Met deze maatregelen en met het uitvoeren van ketentesten doen de diensten het maximale om zorg te dragen dat deze en andere onrechtmatigheden in de toekomst zo veel als mogelijk worden voorkomen.

Voorts is voorzien in concrete en belangrijke waarborgen, onder meer door *logging* ten behoeve van compliance grotendeels af te ronden, waardoor de diensten controle houden op het verwerken van de data en de CTIVD in staat wordt gesteld zo goed mogelijk verscherpt toezicht te houden bij kabelinterceptie, die de komende periode gefaseerd zal worden uitgevoerd. Een aantal compliance-eisen ten behoeve van *logging* en monitoring zijn niet altijd te vatten in systeemoplossingen, deze worden echter in overleg met de CTIVD procesmatig opgelost. Wij vinden het belangrijk dat de CTIVD toezicht kan houden op een manier die passend is voor de dynamische toepassingspraktijk van kabelinterceptie. In dat kader hebben wij de CTIVD verzocht om ons periodiek op de hoogte te stellen van de bevindingen.

Sinds het opstellen van het CTIVD rapport is toestemming voor het toepassen van OOG-interceptie verkregen. Deze toestemming is door de Toetsingscommissie Inzet Bevoegdheden (TIB) inmiddels als rechtmatig beoordeeld. Om een verantwoorde wijze van toepassen te borgen hebben wij de CTIVD verzocht actief mee te kijken met de uitoefening van deze bevoegdheid.

Reflectie van de CTIVD inzake wijziging Wiv 2017

Aard van OOG-interceptie

Tot slot geeft de CTIVD in zijn rapport, met het oog op de wijziging van de Wiv 2017 een reflectie op de aard van OOG-interceptie en in het bijzonder kabelinterceptie. Zo geeft de CTIVD aan dat met name voor de ongekende dreiging geldt dat het moeilijk is te voorspellen waar relevante gegevens zich bevinden. De CTIVD is van oordeel dat de gerichtheid bij kabelinterceptie met name dient te worden gezocht in de toepassing van filters en minder in de keuze van kanalen. De CTIVD acht het van belang dat, mede in het kader van een wijziging van de Wiv 2017, lering wordt getrokken uit de opgedane kennis van en ervaring met kabelinterceptie. Zij concludeert dat de uitleg die in het verleden is gegeven aan onder meer de gerichtheidseis bij kabelinterceptie wringt met de aard van de bevoegdheid, het middel en met de uitvoering in de (technische) praktijk. In het verdere debat moet duidelijker dan tot op heden worden uitgelegd dat deze bevoegdheid per definitie de verwerving van gegevens in bulk betreft en een grote mate van ongerichtheid kent. De aard van het middel en de

inbreuk die het maakt moeten in het openbaar debat worden benoemd en de noodzaak ervan dient te worden beargumenteerd, aldus de CTIVD.

De CTIVD concludeert dat het *snapshotten* dient te worden voorzien van een expliciete wettelijke grondslag. De CTIVD onderschrijft de noodzaak van het *snapshotten* en de analyse van deze gegevens, omdat deze activiteiten in belangrijke mate bijdragen aan de gerichtheid van interceptie ten behoeve van de productiefase. De CTIVD merkt daarbij op dat bij het vormgeven van de wettelijke grondslag het gerichtheidsvereiste moet worden toegepast op een wijze die aansluit bij de aard en het doel van het *snapshotten*.

Wijze van opvolging

Vooruitlopend op een wijziging van de Wiv 2017, verwerkt het kabinet deze conclusie van de CTIVD als volgt. Bij brief d.d. 24 februari 2022 (Kamerstuk 34 588, nr. 91) informeerde ik u al dat enkele knelpunten in het cyberdomein reeds voor afronding van het traject tot wijziging van de Wiv 2017 dienen te worden geadresseerd. Door de toenemende mate van dreigingen in het cyberdomein, iseen tijdelijke wet noodzakelijk om de bescherming van onze nationale veiligheid te kunnen waarborgen. Immers, Nederland en Nederlandse belangen worden in toenemende mate vanuit diverse landen met een offensief cyberprogramma aangevallen in het cyberdomein. Sinds eind vorig jaar wordt derhalve gewerkt aan een voorstel voor een tijdelijke wet die de diensten in staat moet stellen bestaande bevoegdheden, in onderzoeken gericht op landen met een offensief cyberprogramma tegen Nederland en Nederlands belangen, effectiever in te kunnen inzetten. Het gaat hier om een afzonderlijke wet en geen wijziging van de Wiv 2017. Daarin zal ook de door de CTIVD gesignaleerde problematiek inzake *snapshotten* een plaats krijgen.

In het verlengde van de dienaangaande moties[2] van uw Kamer wordt in goed overleg met de TIB en de CTIVD bezien hoe in dit wetsvoorstel het toezicht op de inzet van bevoegdheden waarop de wet van toepassing is, vorm kan worden gegeven waarbij het toezicht geborgd blijft. Het is essentieel voor de legitimiteit van de diensten en het vertrouwen in hun werkzaamheden dat effectief toezicht in de wetgeving is verankerd. Binnen de reikwijdte van dit wetsvoorstel, wordt een sluitend systeem van toezicht opgenomen, zowel vooraf, tijdens als achteraf, dat past bij de dynamiek van cyberoperaties. Vanzelfsprekend worden de bevindingen van de CTIVD in rapport 75 bij het wetsvoorstel betrokken.

Hiermee zullen wij tevens de zorgen zoals benoemd in de op 28 februari 2022 door uw Kamer aangenomen motie van het lid Van der Staaij c.s. adresseren, waarbij de regering wordt verzocht om zo spoedig mogelijk met een voorstel te komen tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
H.G.J. Bruins Slot

De Minister van Defensie,
K.H. Ollongren

[2] Kamerstuk 29 924, nrs. 220, 215 en 218.