

BIJLAGE III: Begrippenlijst

bij het toezichtsrapport over de inzet van kabelinterceptie
door de AIVD en de MIVD

De snapshotfase

CTIVD nr. 75

[Vastgesteld op 26 januari 2022]

CTIVD nr. 75

BIJLAGE III: BEGRIPPENLIJST

bij het toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD

Deze lijst licht een aantal begrippen toe dat wordt gebruikt in het toezichtsrapport. De CTIVD heeft bij de gegeven omschrijvingen geen volledigheid nagestreefd maar geprobeerd de lezer een zo concreet mogelijk beeld te geven van de betreffende begrippen.

Aanbieder	Aanbieder van een communicatiedienst. De natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.
Accesslocatie	Het fysieke ontvangstpunt bij een aanbieder van een communicatiedienst voor geïntercepteerde gegevens. Op deze locatie vindt het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats.
Bijzondere bevoegdheid	Een bevoegdheid van de dienst waarin een specifieke inbreuk op de persoonlijke levenssfeer is geregeld, alsmede de voorwaarden waaronder deze mag worden toegepast. De toepassing van een bijzondere bevoegdheid heeft veelal een geheim karakter. De bijzondere bevoegdheden zijn neergelegd in de artikelen 40 t/m 58 van de Wiv 2017 (bijvoorbeeld tappen en observeren).
Buitenlandse dienst	Een inlichtingen- en/of veiligheidsdienst van een andere staat.
Bulk(dataset)	Een grote gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden.
Ether	In het onderhavige onderzoek duidt deze term niet-kabelgebonden communicatie aan, zoals satelliet- en radiosignalen.
Cyber	Verzamelsnaam voor verschillende activiteiten die te maken hebben met computernetwerken en datastromen.
Cyber Defence	Bescherming tegen digitale dreigingen, zoals cyberaanvallen en malware
Filter	Filteren is het proces dat bepalend is voor het verschil tussen de beschikbare gegevensstromen (communicatie) op de door de diensten gekozen communicatiedragers en de gegevens die uit die stromen uiteindelijk voor het inlichtingenproces worden opgeslagen. Daarmee zijn filters hét instrument om van <i>ongerichte</i>

tot *onderzoeksopdrachtgerichte* interceptie te komen. Filters kunnen worden onderscheiden in positieve en negatieve filters.

Functie- en taakscheiding

Betreft een vorm van compartimentering, waarbij de functie en/of taak bepalend is voor de toegang tot gegevens. Het betreft het bij uitzondering van anderen kennis kunnen nemen van bepaalde gegevens op basis van de taken die aan de functie van deze medewerker zijn toebedeeld.

Gegevensstroom

Gegevens die zich door middel van een verbinding van het ene naar het andere systeem verplaatsen.

Gegevensverwerking

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, aanhef en onder f, van de Wiv 2017).

Geïntegreerde Aanwijzing

De Geïntegreerde Aanwijzing is een aanwijzing van de Raad voor Veiligheids- en Inlichtingendiensten, een onderraad van de ministerraad. De aanwijzing is richtinggevend voor de onderzoeken die de AIVD en de MIVD uitvoeren. Het wordt eens in de vier jaar vastgesteld. De onderzoeksprioriteiten worden aangewezen door de verantwoordelijke ministers van de ministeries die het meest gebruik maken van de AIVD en MIVD-informatie. Het opstellen van de GA gebeurt in overleg tussen de ministeries en de AIVD en de MIVD. De uitwerking van de onderzoeksthema's en de prioritering is opgenomen in de bijlage bij de GA, dat staatsgeheim is.

Gerichtheidsvereiste

Het vereiste dat de toepassing van bijzondere bevoegdheden 'zo gericht mogelijk' dient plaats te vinden.

IP (internetprotocol)

Het protocol dat communicatie tussen computernetwerken faciliteert.

Inlichtingendienst

Een dienst die onderzoek doet naar andere landen om (potentiële) dreigingen voor de eigen nationale veiligheid te onderkennen.

JSCU

Joint Sigint Cyber Unit, gezamenlijke eenheid van de AIVD en de MIVD die zich bezighoudt met de verwerking van gegevens op het gebied van sigint en cyber.

Kabelinterceptie

De toepassing van onderzoeksopdrachtgerichte interceptie op de kabel.

Metadata

Gegevens over communicatie. De metadata van een telefoongesprek zijn bijvoorbeeld de betrokken telefoonnummers, de starttijd en de eindtijd van het gesprek en de gegevens van de betrokken telefoonmasten.

Negatief filter

Het negatief filter bepaalt wat niet wordt opgeslagen. Wanneer er geen criteria in het filter zijn opgenomen, zullen alle gegevens worden opgeslagen. Het filter zorgt ervoor dat op voorhand

bekende/onderkende irrelevante gegevens niet worden opgeslagen. Dit gebeurt aan de hand van kenmerken.

OOG-Interceptie

Onderzoeksopdrachtgerichte interceptie. Bevoegdheid uit artikel 48 Wiv 2017. Deze bevoegdheid is techniekonafhankelijk geformuleerd en kan onder andere doelen op kabelinterceptie en interceptie van de ether.

Onderzoeksopdrachtgericht

Indien niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de inzet van een bevoegdheid of een gegevensverwerking ziet, maar deze wel ten behoeve van een uit de Geïntegreerde Aanwijzing voortvloeiende lopende onderzoeksopdracht 'zo gericht mogelijk' wordt uitgevoerd.

Ongericht

Indien niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de inzet van een bevoegdheid of een gegevensverwerking ziet.

Persoonsgegevens

Gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon (bijvoorbeeld een naam of een foto). Artikel 1, aanhef en onder e, Wiv 2017.

Positief filter

Het positief filter bepaalt wat wordt opgeslagen. Aan de hand van kenmerken wordt bepaald welke gegevens worden opgeslagen. Voorbeelden van kenmerken zijn selectiecriteria behorende bij artikel 50 van de Wiv 2017. Dit kunnen bijvoorbeeld telefoonnummers of e-mailadressen zijn. Indien een kenmerk *matcht* met de geïntercepteerde gegevens wordt de betreffende communicatie opgeslagen

Search

Het verkennen van communicatie als bedoeld in artikel 49 van de Wiv 2017. Search gericht op interceptie, geregeld in artikel 49 lid 1, ziet op het vaststellen van de kenmerken en de aard van telecommunicatie en de identiteit van de bij die communicatie horende persoon of organisatie. Search gericht op selectie, geregeld in artikel 49 lid 2, ziet op het vaststellen en verifiëren van selectiecriteria en op de identificatie van personen of organisaties.

Sigint

Sigint staat voor *signals intelligence*; inlichtingen die verzameld worden door het onderscheppen van elektronische signalen.

Snapshots

Korte integrale opnames (interceptie) van de beschikbare gegevensstromen.

Target

Een persoon of organisatie waarnaar de AIVD of MIVD onderzoek verricht.

Technisch kenmerk

Kenmerk dat herleidbaar is tot verschillende elementen van (tele)communicatie, bijvoorbeeld een telefoonnummer of een e-mailadres.

Veiligheidsdienst

Een dienst die onderzoek doet naar personen en organisaties die mogelijk een gevaar vormen voor het voortbestaan van de democratische rechtsorde, voor de veiligheid of voor andere



gewichtige belangen van de staat, dan wel voor de veiligheid en de paraatheid van de krijgsmacht.

Wiv 2017

Wet op de inlichtingen- en veiligheidsdiensten 2017.

Zo gericht mogelijk

Het tot een minimum beperken van het verwerven en verwerken van niet strikt voor het onderzoek relevante gegevens, gelet op de technische en operationele omstandigheden van de casus.

Zorgplicht

De zorgplicht is neergelegd in artikel 24 van de Wiv 2017. Deze plicht houdt in dat de diensthoofden van de AIVD en de MIVD verantwoordelijk zijn voor de toepassing van technische, personele en organisatorische maatregelen voor een rechtmatige gegevensverwerking.