Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2023-12

De hackbevoegdheid in het buitenland

Een rechtsvergelijkend onderzoek naar wettelijke regelingen en waarborgen omtrent de kwaliteit van gegevens

Wetenschappelijk onderzoek- en kennisinstituut voor het ministerie van Justitie en Veiligheid

Cahier 2023-12

De hackbevoegdheid in het buitenland

Een rechtsvergelijkend onderzoek naar wettelijke regelingen en waarborgen omtrent de kwaliteit van gegevens

J.J. van Berkel
A. van Uden
J.H. Goes

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Alle rapporten van het WODC zijn gratis te downloaden van WODC Repository.

Inhoud

	Samenvatting	**7**
1	**Inleiding**	**18**
1.1	Inleiding	18
1.2	Doelstelling en vraagstelling	19
1.3	Methoden van onderzoek	20
1.3.1	Brede inventarisatie en selectie landen	20
1.3.2	Onderzoeksmethoden	21
1.4	Analyse	24
1.5	Opbouw van het rapport	24
2	**Landenoverzicht**	**25**
2.1	Aanwezigheid hackbevoegdheid en voorwaarden	25
2.2	Waarborgen ten aanzien van de verzamelde gegevens	28
2.2.1	Keuring technische hulpmiddelen en controlerende instantie	29
2.2.2	Documentatie, opslag en rechterlijk toezicht	31
2.2.3	Zitting en inzagerecht	32
	Inleiding op de landenhoofdstukken	**34**
3	**België**	**37**
3.1	Wettelijke regeling	37
3.1.1	Inkijkoperatie	37
3.1.2	Data-interceptie	38
3.2	Bevoegde autoriteiten	39
3.3	Tegen wie	40
3.4	Gevallen	41
3.5	Termijn	41
3.6	Formaliteiten	42
3.7	Technische hulpmiddelen	43
3.8	Waarborgen	43
3.8.1	Betrouwbaarheid en integriteit van gegevens	43
3.8.2	Verslaglegging	44
3.8.3	Samenstelling dossier en inzage	45
3.8.4	Notificatieplicht	47
3.8.5	Extern toezicht	47
3.9	Jurisprudentie	47
3.10	Tot slot	48
4	**Duitsland**	**49**
4.1	Wettelijke regeling	49
4.1.1	Broninterceptie van telecommunicatie	50
4.1.2	Online doorzoeking	50
4.2	Bevoegde autoriteiten	51
4.3	Tegen wie	52
4.4	Gevallen	52
4.5	Termijn	52
4.6	Formaliteiten	53

4.7	Technische hulpmiddelen	54
4.7.1	ZITiS	55
4.8	Waarborgen	55
4.8.1	Technische vereisten	55
4.8.2	Verslaglegging en dossier	59
4.8.3	Extern toezicht	60
4.9	Jurisprudentie	60
4.10	Tot slot	61
4.10.1	Voorafgaand aan een inzet	61
4.10.2	Tijdens en na afloop van een inzet	62
5	**Frankrijk**	**63**
5.1	Wettelijke regeling	63
5.2	Bevoegde autoriteiten	64
5.3	Tegen wie	65
5.4	Gevallen	65
5.5	Termijn	65
5.6	Formaliteiten	66
5.6.1	Gebruik technische hulpmiddelen	66
5.7	Inzet technische hulpmiddelen vastleggen computergegevens	67
5.8	Waarborgen	67
5.8.1	Magistratelijke toetsing	67
5.8.2	Nationale technische dienst voor gerechtelijke vastlegging (STNCJ)	68
5.8.3	Notificatieplicht en recht op inzage	68
5.9	Jurisprudentie	69
5.10	Tot slot	69
6	**Zweden**	**71**
6.1	Wettelijke regeling	71
6.2	Bevoegde autoriteiten	72
6.3	Tegen wie	72
6.4	Gevallen	73
6.5	Termijn	73
6.6	Formaliteiten	73
6.6.1	Publieke vertegenwoordiger	74
6.7	Technische hulpmiddelen	74
6.8	Waarborgen	75
6.8.1	Zorgvuldigheidsvereisten	75
6.8.2	Commissie voor Veiligheid en Integriteitsbescherming (SIN)	75
6.8.3	Interne richtlijnen heimelijke gegevensuitlezing	76
6.8.4	Notificatieplicht en recht op inzage	77
6.9	Jurisprudentie	78
6.10	Tot slot	79
7	**Zwitserland**	**80**
7.1	Wettelijke regeling	80
7.2	Bevoegde autoriteiten	81
7.3	Tegen wie	82
7.4	Gevallen	83
7.5	Termijn	83
7.6	Formaliteiten	83
7.7	Technische hulpmiddelen	84

7.8	Waarborgen	85
7.8.1	Volledige vastlegging & veilig versturen gegevens	85
7.8.2	Openbaarmaking broncode	86
7.8.3	Speciale dienst en keuring	86
7.8.4	Andere technische en organisatorische maatregelen	87
7.8.5	Verslaglegging en dossier	87
7.8.6	Notificatieplicht	88
7.9	Jurisprudentie	88
7.10	Tot slot	88
8	**Conclusie**	**91**
8.1	Belangrijkste (knel-)punten keuring technische hulpmiddelen in Nederland	91
8.2	Algemene observaties buitenland	93
8.3	Landenvergelijking	94
8.3.1	Waarborgen voorafgaand aan inzet bevoegdheid	94
8.3.2	Waarborgen tijdens inzet bevoegdheid	96
8.3.3	Waarborgen na inzet bevoegdheid	97
8.4	Slotbeschouwing	100
	Summary	**105**
	Literatuur	**116**
Bijlage 1	**Bronnenoverzicht**	**122**
Bijlage 2	**Landenoverzicht hackbevoegdheid**	**123**
Bijlage 3	**Landenoverzicht waarborgen verzamelde gegevens**	**129**
Bijlage 4	**Uitgebreide landbeschrijving Nederland**	**146**
Bijlage 5	**Samenstelling begeleidingscommissie**	**158**

Samenvatting

Op 1 maart 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. Een onderdeel van deze wet is de introductie van de 'hackbevoegdheid' van de politie. Op basis van de nieuwe artikelen 126nba, 126uba, 126zpa in het Wetboek van Strafvordering (Sv) wordt het voor daartoe geautoriseerde opsporingsambtenaren onder bepaalde voorwaarden mogelijk om op afstand heimelijk binnen te dringen in een geautomatiseerd werk en daarin onderzoek te doen. De onderzoekshandelingen kunnen worden verricht met een technisch hulpmiddel. In beginsel moet een technisch hulpmiddel voorafgaand aan het gebruik ervan worden gekeurd en goed bevonden worden door een onafhankelijke keuringsdienst (de Keuringsdienst), om de betrouwbaarheid, herleidbaarheid en integriteit van het bewijs te borgen.

De Inspectie Justitie & Veiligheid (hierna Inspectie) houdt toezicht op de uitvoering van de hackbevoegdheid. In haar eerste Verslag in 2020 concludeerde zij dat de inzet van technische hulpmiddelen bij de hackbevoegdheid en de keuring van deze hulpmiddelen nog niet verliepen zoals volgens het wettelijk kader was bedoeld. In zijn reactie op het eerste Verslag van de Inspectie heeft de toenmalig Minister van Justitie en Veiligheid aangegeven dat hij zou laten onderzoeken met welke waarborgen het gebruik van technische hulpmiddelen in het buitenland is omkleed. Onderhavig rapport is het resultaat van dit onderzoek. Dit rapport vormt tevens een aanvulling op de eerder verschenen evaluatie naar het gebruik van de hackbevoegdheid in Nederland, uitgevoerd door het WODC.

Vraagstelling

De centrale onderzoeksvraag van dit onderzoek is als volgt:

Met welke waarborgen is in het buitenland de hackbevoegdheid, meer in het bijzonder het gebruik van technische hulpmiddelen omkleed en hoe verhoudt zich dat tot de Nederlandse situatie?

De centrale onderzoeksvraag wordt beantwoord aan de hand van de volgende deelvragen:

1 Welke landen kennen een 'hackbevoegdheid' en op basis van welke wettelijke grondslag kunnen buitenlandse politiediensten in hun eigen land gebruikmaken van de hackbevoegdheid?
2 Welke wettelijke voorwaarden gelden er in het buitenland voor politiediensten om de hackbevoegdheid in te kunnen zetten?
3 In hoeverre kennen andere landen een keuring van technische hulpmiddelen en wat is hierover in wet- en regelgeving vastgelegd?
4 In hoeverre gelden er nog andere regels om de betrouwbaarheid, herleidbaarheid en integriteit van de gegevens, die zijn verkregen met behulp van de inzet van technische hulpmiddelen, te waarborgen?
5 Hoe verhoudt de werkwijze in het buitenland zich tot de Nederlandse manier van werken met betrekking tot het keuren van technische hulpmiddelen en eventuele andere waarborgen om de betrouwbaarheid, integriteit en herleidbaarheid van gegevens te realiseren?

Methoden van onderzoek

Voor het onderzoek is een brede inventarisatie gemaakt om in kaart te brengen welke landen een wettelijke hackbevoegdheid kennen. Om van een hackbevoegdheid te kunnen spreken hanteerden we als uitgangspunt dat de hackbevoegdheid heimelijk en op afstand wordt uitgevoerd. In het kader van de brede inventarisatie zijn nagenoeg alle Europese landen bekeken plus de Verenigde Staten, Canada en Australië. Op basis van de brede inventarisatie is een selectie van vijf landen gemaakt die nader zijn bestudeerd: België, Duitsland, Frankrijk, Zweden en Zwitserland.
Om de onderzoeksvragen te beantwoorden zijn verschillende onderzoeksmethoden gebruikt: documentstudie (wet- en regelgeving en relevante (grijze) literatuur), schriftelijke vragenlijsten en interviews.

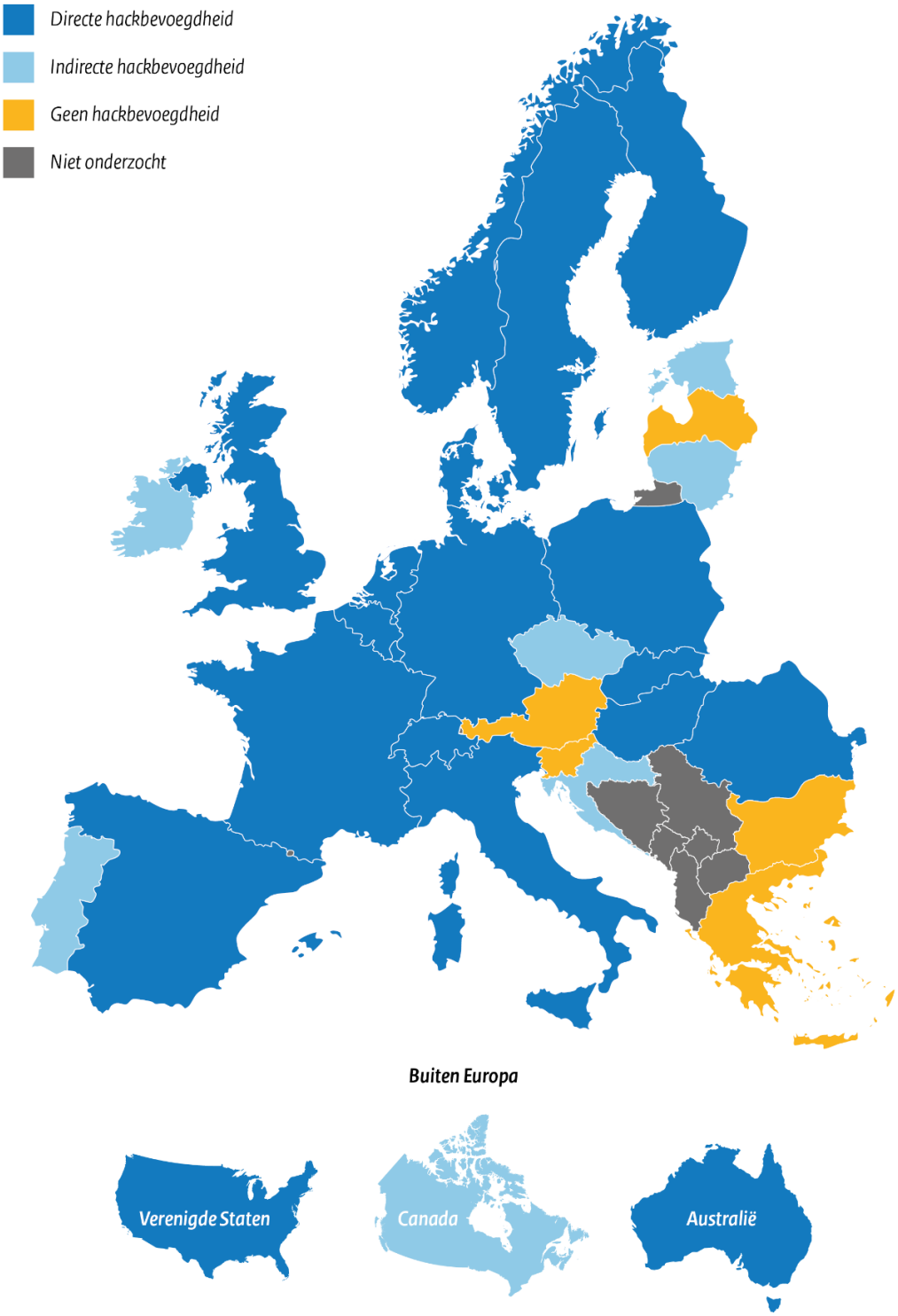
Brede inventarisatie

Op basis van de brede inventarisatie is in dit rapport een aantal onderwerpen besproken. In deze samenvatting wordt aandacht besteed aan de aanwezigheid van een hackbevoegdheid, de keuring van technische hulpmiddelen en de aanwezigheid van een controlerende instantie, de waarborgen voor documentatie, opslag en rechterlijk toezicht, en de notificatieplicht en het inzagerecht.

Aanwezigheid hackbevoegdheid

Figuur S1 op de volgende pagina geeft weer of een land een wettelijke hackbevoegdheid voor de politie kent en zo ja, of dit een directe of indirecte bevoegdheid is. Van een directe bevoegdheid is sprake als de wet expliciet de mogelijkheid noemt een geautomatiseerd werk heimelijk en op afstand binnen te dringen en daarbinnen één of meerdere onderzoekshandelingen te verrichten. Van een indirecte bevoegdheid is sprake als de hackbevoegdheid deel uitmaakt van een algemene bepaling. Dit gaat bijvoorbeeld om een interceptiebevoegdheid, waarbij in de wetstekst niet specifiek de hackbevoegdheid wordt genoemd, maar de bevoegdheid wel voor dat doel kan worden gebruikt.

Figuur S1 Landenoverzicht hackbevoegdheid



Kaarten zijn bewerkingen van werken van Maix (Europa; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; publiek domein) en Rycherr (Australië; CC BY-SA 4.0 en eerdere versies).

Keuring technische hulpmiddelen en controlerende instantie

Geen enkel land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keurings-protocol, de technische hulpmiddelen dient te onderzoeken. Sommige landen kennen wel een testprocedure, maar dit wordt niet uitgevoerd door een onafhankelijke keuringsdienst. Verder geldt voor de overige landen die een keuring of testprocedure kennen, dat onbekend is hoe de procedure eruitziet. Duitsland vormt hierop een uitzondering. Ook daar is niet volledig duidelijk hoe de keuring eruitziet, maar het is wel bekend dat deze gebaseerd is op een speciaal daarvoor geformuleerde SLB-richtlijn.

Het toezicht op de uitvoering van de bevoegdheid door een onafhankelijke instantie is in het buitenland beperkt (de zittingsrechter buiten beschouwing gelaten). Voor Australië, Denemarken, Noorwegen, het Verenigd Koninkrijk en Zweden geldt dat een vorm van toezicht plaatsvindt op de uitvoering van de bevoegdheid door een onafhankelijke instantie. Daarnaast bestaat in Duitsland een instantie die, vanwege haar technische expertise, adviseert over de inzet en ontwikkeling van technische hulpmiddelen. Frankrijk kent een specifieke instantie die verantwoordelijk is voor het ontwerp, de aansturing en de implementatie van technische hulpmiddelen die gebruikt worden voor de hackbevoegdheid.

Waarborgen voor documentatie, opslag en rechterlijk toezicht

Ten aanzien van het documenteren en loggen van uitvoeringshandelingen geldt dat in vrijwel alle landen een vorm van documentatie vereist is. Dit betekent dat op zijn minst een proces-verbaal moet zijn opgesteld waarin alle handelingen staan gedocumenteerd. Sommige landen gaan een stap verder, omdat daar alle handelingen moeten worden gelogd. Voor vijf landen is gedurende ons onderzoek niet duidelijk geworden of daar eisen worden gesteld aan het documenteren en loggen van uitvoeringshandelingen.

In België, Frankrijk, Kroatië, Portugal en Spanje vindt *gedurende* de inzet van de bevoegdheid rechterlijk toezicht plaats. Dit betekent dat de politie tussentijds aan de rechter die de machtiging heeft verleend statusupdates moet geven over de voort-gang. In sommige gevallen kan de rechter op basis daarvan besluiten de toestemming voor de inzet van de bevoegdheid in te trekken. Voor de overige landen geldt dat – voor zover bekend – geen tussentijds rechterlijk toezicht plaatsvindt.

Twintig landen kennen in de wet opgenomen waarborgen ten aanzien van de opslag van gegevens die zijn verkregen met de hackbevoegdheid. Hierbij gaat het onder meer om het verzegeld opslaan van de gegevens of het opslaan van de gegevens in een beveiligde omgeving. Voor de overige landen geldt dat er niets is opgenomen in de wet of dat ons niet duidelijk is geworden of landen (informele) waarborgen kenden.

Notificatieplicht en inzagerecht

In dertien landen is een notificatieplicht opgenomen in de wet. Dat betekent dat personen van wie het geautomatiseerd werk is binnengedrongen binnen een bepaalde termijn geïnformeerd moeten worden dat de bevoegdheid is ingezet. In de helft van

deze landen kan notificatie worden uitgesteld of soms zelfs achterwege blijven als opsporingsbelangen in het gedrang kunnen komen. Voor vrijwel alle landen geldt dat de verdachte wordt genotificeerd, als een zaak ter zitting komt. Verder is in zeventien landen het recht op inzage tot de verkregen gegevens expliciet opgenomen in de wet. In veel gevallen kan de verdediging een kopie van de verkregen gegevens ontvangen. Bij de overige landen is in onze inventarisatie niet naar voren gekomen of voor de bevoegdheid een specifieke wettelijke bepaling is opgenomen ten aanzien van het recht op inzage.

Verdiepende landenvergelijking

In dit onderzoek is ook een aantal landen diepgaander bestudeerd. Deze landen zijn onderling en met Nederland vergeleken. Daarom volgt eerst een beschrijving van de belangrijkste knelpunten in Nederland. Daarna volgt de landenvergelijking.

Belangrijkste (knel-)punten keuring technische hulpmiddelen in Nederland

De Nederlandse wetgever heeft ervoor gekozen om bij de introductie van de hackbevoegdheid het keuringssysteem van technische hulpmiddelen te volgen dat gebruikt wordt voor al bestaande (bijzondere) opsporingsbevoegdheden. Voor de hackbevoegdheid is een apart besluit genaamd 'Besluit onderzoek in een geautomatiseerd werk' (hierna Besluit) ontworpen. In dit Besluit worden diverse eisen gesteld aan een technisch hulpmiddel, waaronder eisen die gericht zijn op de integriteit, herleidbaarheid en betrouwbaarheid (hierna kwaliteit) van de verzamelde gegevens. De Keuringsdienst voert de keuringen in Nederland uit en zij hanteert daarbij een keuringsprotocol dat gebaseerd is op diverse artikelen uit het Besluit. In principe moet de politie gebruikmaken van een technisch hulpmiddel dat vooraf (goed-)gekeurd is. Hiervoor geldt een aantal uitzonderingen: (1) een technisch hulpmiddel kan achteraf gekeurd worden; (2) er kan worden overgegaan op een handmatige inzet; of (3) de officier van justitie oordeelt dat het middel 'naar zijn aard' niet te keuren is.

Uit de Verslagen van de Inspectie en het eerste evaluatierapport van het WODC blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk bedoeld. Het inzetten van een vooraf goedgekeurd technisch hulpmiddel gebeurt niet of nauwelijks en voor de opsporingspraktijk vormt de keuring een belangrijk knelpunt. Verschillende aspecten spelen hierbij een rol:

- De doorlooptijd van een keuring neemt relatief veel tijd in beslag, tenminste vier maanden. Die tijd past niet altijd bij de snelheid die nodig kan zijn binnen een opsporingsonderzoek.
- Een technisch hulpmiddel aanpassen dat nog niet goedgekeurd is, vereist altijd een nieuwe keuring en kost dus tijd.
- Het Besluit vereist, en daardoor ook de Keuringsdienst, dat een technisch hulpmiddel aan alle eisen dient te voldoen, wil het technisch hulpmiddel goedgekeurd worden. De opsporingspraktijk stelt echter vragen over het nut en de noodzakelijkheid van (het voldoen aan) alle eisen.
- De inzet van technische hulpmiddelen gebeurt in een omgeving die Digit, het politieteam dat de bevoegdheid uitvoert, niet altijd onder controle heeft. Digit heeft bijvoorbeeld géén invloed op wat een verdachte met zijn of haar geautomatiseerd werk doet. Handelingen van de eigenaar van het geautomatiseerd werk kunnen de kwaliteit van de verzamelde gegevens aantasten. Digit zou zich meer willen richten

op het maken van een risicoanalyse met betrekking tot het gebruikte technisch hulpmiddel en op de bewijswaarde van de verzamelde gegevens.
- Bij een risicoanalyse gaat het om de vraag hoe groot het risico is dat de kwaliteit van de gegevens in het gedrang komt als een technisch hulpmiddel wordt gebruikt dat niet aan alle eisen voldoet.
- Het is verder de vraag wat het gebruik van een technisch hulpmiddel, dat niet aan alle eisen voldoet, betekent voor de bewijswaarde van de verzamelde gegevens. Zeker wanneer de gegevens slechts een deel vormen van het bewijs dat verzameld is.

In de opsporingsonderzoeken waarin de hackbevoegdheid in Nederland is ingezet werd in de meerderheid van de onderzoeken gebruikgemaakt van een commercieel product. Ook hiervoor geldt dat geen gebruik is gemaakt van een vooraf goedgekeurd hulpmiddel. Sterker nog, het product is nooit ter keuring aangeboden, omdat de Digitofficier van justitie, de landelijk officier die de bevoegdheid in portefeuille heeft, oordeelde dat de aard van dit hulpmiddel zich verzet tegen een keuring. Daarbij maakte de officier van justitie gebruik van een uitzonderingsgrond in het Besluit. Dit product kan overigens onder het huidige keuringsregime ook niet goedgekeurd worden. Een aantal punten maakt dat dit product naar zijn aard niet te keuren is en/of nooit goedgekeurd zal worden:
- Commerciële middelen worden relatief vaak geüpdatet. De vraag is welke versie(-s) de Keuringsdienst moet keuren. Mocht dit bij alle versies noodzakelijk zijn, dan past dat niet bij de doorlooptijd die een keuring doorgaans in beslag neemt in relatie tot de termijn waarbinnen een inzet plaats moet vinden.
- De exacte werking van dit soort middelen is voor de gebruikers ervan een 'zwarte doos'. Daardoor krijgt de Keuringsdienst geen inzage in de precieze werking en kan geen volledige keuring plaatsvinden.
- Een leverancier heeft te allen tijde toegang tot zijn product, bijvoorbeeld voor het plegen van onderhoud. Daardoor krijgt de Keuringsdienst geen exclusieve toegang tot het middel, hetgeen voor haar een vereiste is om de keuring te kunnen doen. Geen exclusieve toegang betekent geen goedkeuring, omdat niet uitgesloten kan worden dat een andere partij dan de verdachte en de politie toegang heeft gehad tot de verzamelde gegevens. Dat betekent dat de betrouwbaarheid en de integriteit van de gegevens niet volledig gegarandeerd kunnen worden.

Het niet uitvoeren van een keuring leidt ertoe dat in een meerderheid van de opsporingsonderzoeken niet voldaan wordt aan een belangrijke waarborg ten aanzien van de kwaliteit van de verzamelde gegevens. Daarbij dient opgemerkt te worden dat in deze situatie wel aanvullende technische en tactische waarborgen worden getroffen om de betrouwbaarheid van het bewijs te kunnen garanderen. Deze tactische waarborgen worden tijdens de keuring niet meegenomen.

Landenvergelijking

In ons onderzoek zijn vijf landen meer diepgaand bestudeerd: België, Duitsland, Frankrijk, Zweden en Zwitserland. Om de landen te vergelijken is ten aanzien van de waarborgen onderscheid gemaakt tussen drie fases tijdens de inzet van de hackbevoegdheid: de fase voorafgaand aan de inzet, tijdens de inzet en na de inzet van de hackbevoegdheid.

Waarborgen voorafgaand aan inzet bevoegdheid

Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. De wijze waarop verschilt echter per land. Nederland kent de meest gedetailleerde *beschreven* keuring van technische hulpmiddelen. De wijze waarop Duitsland de criteria heeft beschreven lijkt het meest in de buurt te komen bij de wijze waarop Nederland dat heeft gedaan. De Duitse keuring is gebaseerd op de SLB-richtlijn, waarbij de volgende thema's centraal staan: beschermingsdoelen en veiligheidsmaatregelen, werkprocessen en procedures, leveranciers en testbeleid. Het hanteren van de richtlijn is geen wettelijk vereiste, maar geldt als leidraad. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten (denk aan systeemcomponenten zoals hard- en software, applicaties, organisatorische of personele aangelegenheden) risico opleveren. De resultaten van die risicoanalyse, de vaststelling van de beschermingsbehoeften en de daaruit voortvloeiende gevolgen en de uitvoering ervan, worden vastgelegd in een IT-beveiligingsconcept. Zowel leveranciers van software als gebruikers van de software dienen zich aan dit concept te conformeren. In de overige landen is niet bekend welke criteria deel uitmaken van de keuring.

In Nederland wordt de keuring uitgevoerd door de Keuringsdienst. De Keuringsdienst is onafhankelijk, maar valt formeel onder hetzelfde organisatieonderdeel van de Nationale Politie als waar het team toebehoort dat de bevoegdheid uitvoert. In Frankrijk voert een specifieke overheidsinstantie genaamd STNCJ de keuring uit. Deze instantie is ook verantwoordelijk voor de uitvoering van de bevoegdheid. In beide landen kan door de wijze waarop de taken zijn belegd de vraag rijzen hoe onafhankelijk de keuring is. Dit geldt in het bijzonder voor Frankrijk, waarbij het ook daadwerkelijk dezelfde organisatie is die uitvoert en keurt. In de andere landen toetst de politie zelf. Interessant om op te merken is dat in Frankrijk en Zwitserland de 'keurder' en uitvoerder dezelfde partij zijn. In deze landen wordt dit niet als problematisch gezien en wordt aangenomen dat de partijen in principe vertrouwenswaardig handelen. In Zweden vindt – voor zover bekend – geen formele keuring plaats. Wel wordt daar later in het proces van het hacken – als de gegevens op de systemen van de politie staan – veelal gebruikgemaakt van gestandaardiseerde software. Dit is bijvoorbeeld software gecertificeerd door andere politiediensten, zoals de Nederlandse politie.

Waarborgen tijdens inzet bevoegdheid

De waarborgen tijdens de inzet van de bevoegdheid verschillen per land. Gangbare waarborgen in deze fase zijn vormen van logging, verslaglegging, het gebruik van een beveiligd transport van gegevens afkomstig uit het geautomatiseerd werk en het opslaan van de gegevens in een beveiligde omgeving.

In België en Frankrijk vindt gedurende de inzet van de bevoegdheid rechterlijk toezicht plaats. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de bevoegdheid. Indien de uitvoering van de bevoegdheid niet conform de voorwaarden van de toestemming plaatsvindt, kan de inzet van de bevoegdheid worden stopgezet. Daarbij moet worden opgemerkt dat de rechter afhankelijk is van de informatie die de politie of de officier van justitie tussentijds verstrekt of kan verstrekken. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk voor zal zorgen dat een inzet tussentijds beëindigd kan worden. Het rechterlijk toezicht in deze landen gaat verder dan de rol van de rechter-

commissaris in Nederland, die in principe alleen voorafgaand aan een inzet (of een verlenging ervan) meekijkt. Wel kent Nederland nog het toezicht door de Inspectie Justitie en Veiligheid.

Waarborgen na inzet bevoegdheid

De meest voorkomende waarborgen hebben betrekking op de notificatie van de inzet van de bevoegdheid aan de verdachte(n) of betrokkene(n), de inhoudelijke behandeling tijdens de zitting en het inzagerecht van de verdachte. Notificatie is niet in alle landen gegarandeerd, omdat dit soms achterwege kan blijven indien het risico bestaat dat lopende opsporingsbelangen worden geschaad. In België moet op basis van de wet altijd genotificeerd worden. Frankrijk is het enige land waarin een verdachte niet genotificeerd hoeft te worden. Uiteraard geldt dat indien de gehackte gegevens deel uitmaken van de bewijsvoering de verdachte door inzage in het dossier indirect wordt genotificeerd. Welke informatie in het dossier wordt opgenomen, en tot hoever het inzagerecht strekt, is niet voor alle landen duidelijk geworden. Wel komt naar voren dat in de meeste gevallen de verdediging een kopie ontvangt van (een selectie van) de gegevens die verzameld zijn met de hackbevoegdheid.

Op basis van de interviews blijkt dat nog weinig jurisprudentie beschikbaar is waarin de kwaliteit van de gegevens, verzameld met behulp van de hackbevoegdheid, ter discussie is gesteld. Dat maakt het lastig om de vraag te beantwoorden in welke mate een zittingsrechter de inzet van de bevoegdheid en de kwaliteit van de gegevens toetst. De jurisprudentie die ons wel bekend is gaat veelal over zaken waarin bewijs wordt gebruikt gebaseerd op gegevens van de communicatiedienst Encrochat. De Franse autoriteiten hebben deze communicatie kunnen onderscheppen. In veel landen zijn Encrochat-gegevens gebruikt als bewijs. Bij de behandeling van deze zaken stond echter vooral de vraag centraal of het verkregen bewijs rechtmatig was en niet de vraag wat de kwaliteit van de verzamelde gegevens was. Voor zover bekend is alleen in Zweden en Frankrijk de kwaliteit van gegevens ter discussie gesteld. In Zweden verwierp de rechtbank relatief eenvoudig de geuite bezwaren ten aanzien van de kwaliteit van de gegevens. Opvallender is een arrest van oktober 2022 uit Frankrijk. Daarin concludeert de rechter dat, bij gebrek aan een certificaat van waarheidsgetrouwheid, het niet wordt geaccepteerd dat niets gedeeld wordt over de wijze waarop het bewijs verkregen is.. Dit geldt echter alleen als de verzamelde gegevens versleuteld zijn. Het ligt voor de hand dat de politie de bevoegdheid juist inzet om ontsleutelde berichten (live) te kunnen inzien. In deze gevallen is een certificaat dus niet benodigd.

Een ander opvallend punt ten aanzien van de waarborgen na afloop van de inzet is de wettelijke bepaling in Zwitserland dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Voorafgaand aan de inzet moet ook worden verzekerd dat de leverancier geen toegang kan krijgen tot de gegevens. Het prijsgeven van de broncode en de toegangsbeperking vallen op, omdat beide punten in Nederland een belangrijk obstakel vormen om commerciële middelen (goed) te keuren. Een relevante vraag, die helaas niet beantwoord kan worden op basis van ons onderzoek, is daarom in hoeverre beide vereisten uiteindelijk afgedwongen kunnen worden in Zwitserland.

Ten slotte valt op dat Zweden het enige van de vijf landen is dat een specifieke toezichthouder (SIN) kent die toezicht houdt op de bevoegdheid. De rol van SIN ten aanzien van de inzet van technische hulpmiddelen voor de hackbevoegdheid is nog in

ontwikkeling. Het toezicht richt zich vooralsnog vooral op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid). SIN heeft echter de bevoegdheid om ook naar de technische hulpmiddelen zelf te kijken.

Scenario's

Op basis van ons onderzoek hebben wij een drietal scenario's geformuleerd die mogelijk een aanvulling kunnen bieden op de wijze waarop in Nederland met technische hulpmiddelen en gegevens, verzameld middels de hackbevoegdheid, wordt omgegaan. Deze scenario's worden in onderstaande tekst beschreven.

Scenario 1: Broncode en controle op toegang gegevens

In ons onderzoek komt naar voren dat het in Zwitserland wettelijk verplicht is dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Daarnaast moet verzekerd worden dat de leverancier geen toegang kan krijgen tot de gegevens wanneer deze verzameld worden. Juist deze twee punten vormen een belangrijk obstakel in Nederland om commerciële technische hulpmiddelen te keuren. Het is niet duidelijk geworden in hoeverre de Zwitserse autoriteiten daadwerkelijk beide vereisten hebben kunnen realiseren. Voor zover bekend is er nog geen zaak geweest waarin daadwerkelijk om de broncode is gevraagd. De leverancier heeft er in beginsel geen baat bij om inzage te geven in zijn broncode. De werkwijze van de software is een goed bewaard geheim. Echter, als Zwitserland een werkbare oplossing heeft kunnen vinden, is het voor de politie, het Openbaar Ministerie en beleidsmakers in Nederland waardevol om te verkennen hoe dit op een soortgelijke manier gerealiseerd kan worden. Daarmee zouden twee belangrijke knelpunten bij de keuring in Nederland opgeheven kunnen worden.

Scenario 2: Veranderende rol toezicht

Gedurende het Nederlandse wetstraject is het toezicht tijdens de inzet van de bevoegdheid een belangrijk discussiepunt geweest. Extra toezicht zou nodig zijn omdat rechters niet altijd in staat zouden zijn om het verzamelde bewijs goed te beoordelen. Ook was de verwachting dat een (groot) deel van de zaken nooit door een zittingsrechter behandeld zou worden. Er is geopperd om een vergelijkbaar orgaan in het leven te roepen als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Verschillende auteurs hebben in de loop van de tijd gewezen op het belang van (extra) toezicht, dan wel een andere vorm van toezicht. De wetgever heeft uiteindelijk niet gekozen voor een commissie vergelijkbaar met de CTIVD. Argumenten hiervoor waren het reeds bestaande toezicht door een rechter-commissaris en het toezicht door de Centrale Toetsingscommissie van het Openbaar Ministerie. In plaats daarvan is gekozen voor de Inspectie Justitie en Veiligheid, die toezicht houdt op zaken die wel en niet aan de rechter worden voorgelegd.
Op basis van ons onderzoek nemen wij geen positie in ten aanzien van deze discussie. Wel is het relevant om te noemen dat, als ten aanzien van de hackbevoegdheid de rol van het toezicht verder wordt verkend, een aantal landen uit onderhavig onderzoek mogelijke handvatten kan bieden.

Ten eerste is in dit kader relevant dat in België en Frankrijk een onderzoeksrechter toezicht houdt op de uitvoering van de bevoegdheid. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de

bevoegdheid. Indien nodig kan de rechter besluiten de inzet van de bevoegdheid stop te zetten. Dit toezicht gaat verder dan de rol van de rechter-commissaris, die in principe alleen voorafgaand aan een inzet controle uitoefent. De werkwijze in België en Frankrijk ondervangt het probleem dat een deel van de zaken niet door de zittingsrechter wordt behandeld. Als kanttekening moet worden opgemerkt dat de rechter afhankelijk is van de informatie die hij of zij verstrekt krijgt. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk toe leidt dat gedurende een inzet een inhoudelijke toets plaatsvindt. Wel biedt het een perspectief dat afwijkt van de Nederlandse systematiek, waarin de rechter-commissaris voorafgaand toestemming verleent en daarna in principe niet meer toeziet op de uitvoering van de bevoegdheid.

Ten tweede is de Zweedse toezichthouder (SIN) relevant. Deze toezichthouder houdt specifiek toezicht op de uitvoering van de hackbevoegdheid. Hij lijkt daarmee op de mogelijke introductie van een commissie naar voorbeeld van de CTIVD. SIN richt zich vooralsnog primair op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid) en houdt zowel toezicht op de activiteiten van de politie als van het Openbaar Ministerie. Hiermee onderscheidt hij zich van de taken van de Inspectie in Nederland die alleen toezicht houdt op de politie. Daarnaast kan SIN op verzoek en uit eigen beweging publiekelijk uitspraken doen in individuele zaken. Doordat SIN zich zowel richt op de juridische als op de procesmatige aspecten worden de eerder aangehaalde problemen ondervangen dat niet alle zaken voor een zittingsrechter komen en dat de rechter niet altijd voldoende in staat zou zijn al het bewijs goed te beoordelen.

Scenario 3: Keuring op maat

Zoals reeds besproken vormt de keuring in Nederland een belangrijke waarborg bij de inzet van technische hulpmiddelen en de kwaliteit van de gegevens die met het middel worden verzameld. In de praktijk blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk is bedoeld. Er wordt voornamelijk gebruikgemaakt van niet vooraf goedgekeurde technische hulpmiddelen en technische hulpmiddelen die naar hun aard niet te keuren zijn. Opvallend is dat in het buitenland de waarborgen rondom technische hulpmiddelen en de kwaliteit van gegevens wettelijk minder gedetailleerd beschreven zijn dan in Nederland. In dat opzicht is het in het buitenland gemakkelijker om de bevoegdheid in te zetten. Ook valt op dat in die landen (vooralsnog en voor zover ons bekend) niet of nauwelijks jurisprudentie beschikbaar is die het gebruik van de hackbevoegdheid in deze landen ter discussie stelt. Dat betekent overigens niet dat het bewijs van de hackbevoegdheid altijd zomaar geaccepteerd zal worden. In veel landen is de hackbevoegdheid relatief nieuw en zal het gebruik ervan en een oordeel daarover zich nog verder ontwikkelen. Het valt dan ook niet uit te sluiten dat in de toekomst alsnog uitspraken volgen die gevolgen hebben voor het huidig wettelijke kader in deze landen. Dat neemt niet weg dat het interessant is om te constateren dat in de verschillende landen niet de keuze is gemaakt om de kwaliteit van de gegevens te controleren op een wijze waarop Nederland dat doet. En dat de buitenlandse manier van werken voor zover bekend vooralsnog niet tot wezenlijke discussies in de rechtbank heeft geleid. Daarom hebben we een derde scenario opgenomen waarin oog is voor meer maatwerk ten aanzien van de keuringseisen, waarbij aandacht is voor aanvullende tactische en technische waarborgen. Dit scenario verkent (a) het gebruik van een risicoanalyse in de keuring en (b) de vraag in hoeverre aanvullende tactische en technische maatregelen voldoende gewaarborgd zijn.

Scenario 3a: Risicoanalyse in de keuring

In Duitsland speelt het maken van risicoanalyses een rol wanneer het gaat om de aanschaf en het gebruik van technische hulpmiddelen. In een SLB-richtlijn worden diverse onderwerpen genoemd waarmee rekening zou moeten worden gehouden als het gaat om technische hulpmiddelen, zoals het testbeleid. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten risico lopen en welke aanvullende maatregelen nodig zijn. De verschillende betrokken partijen dienen zich hieraan te conformeren. In Nederland geeft de uitvoerende partij (Digit) aan dat de Keuringsdienst (en het onderliggende keuringsprotocol) onvoldoende rekening houdt met het feit dat zij ook zou kunnen werken op basis van risicoanalyses, namelijk wat betreft de maatregelen die zij neemt wanneer zij een inzet doet met een technisch hulpmiddel. Juist deze risicoanalyse lijkt een meer centrale plek te hebben in Duitsland. Daarom zou de werkwijze in Duitsland nader verkend kunnen worden om te zien wat daaruit geleerd kan worden voor de Nederlandse situatie.

Scenario 3b: Borging aanvullende tactische waarborgen in Nederland

Zoals opgemerkt, wordt in Nederland op dit moment primair gebruikgemaakt van technische hulpmiddelen waarvan de officier van justitie oordeelt dat ze naar hun aard niet te keuren zijn. In deze situatie worden tactische en technische maatregelen getroffen om de kwaliteit van de gegevens te waarborgen. Voor nu zijn er geen aanwijzingen dat het gebruik van commerciële producten beëindigd zal worden. De huidige minister ziet deze als 'een realiteit waar we mee te dealen hebben', zo blijkt uit een Commissiedebat op 7 juli 2022. Het gebruik van risicoanalyses beschreven in scenario 3a kan een handvat bieden om juiste aanvullende maatregelen te treffen om de kwaliteit van de gegevens te waarborgen. Indien de werkwijze met commerciële producten eerder regel dan uitzondering blijft en exact op dezelfde manier gewerkt zal blijven worden, is het ook van belang de rol van het Openbaar Ministerie ten aanzien van de aanvullende (tactische) waarborgen tegen het licht te houden. Op dit moment is het de enige die voorafgaand aan een inzet de tactische waarborgen bekijkt. Een tactisch officier van justitie die het opsporingsonderzoek leidt is in principe eindverantwoordelijk voor deze waarborgen. Deze worden ook bekeken door de Digit officier van justitie en de Centrale toetsingscommissie van het Openbaar Ministerie. Vanwege enkel de betrokkenheid van het Openbaar Ministerie en geen andere onafhankelijke instantie, is het nuttig om te verkennen welke andere partij (aanvullend) kan controleren of deze maatregelen toereikend zijn, zeker in gevallen dat een zittingsrechter een zaak niet zal behandelen.

1 Inleiding

1.1 Inleiding

Op 1 maart 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. Een onderdeel van deze wet is de introductie van de 'hackbevoegdheid' van de politie. Op basis van de nieuwe artikelen 126nba, 126uba, 126zpa in het Wetboek van Strafvordering (Sv) wordt het voor daartoe geautoriseerde opsporingsambtenaren onder bepaalde voorwaarden mogelijk om op afstand heimelijk binnen te dringen in een geautomatiseerd werk en daarin onderzoek te doen. Een geautomatiseerd werk is 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken'.[1] Voorbeelden van geautomatiseerde werken zijn: smartphones, laptops en routers.[2] Na het binnendringen kan de politie onderzoekshandelingen verrichten, onder andere het uitvoeren van een bevel zoals bedoeld in de artikelen 126l Sv (direct afluisteren) en 126m Sv (aftappen van communicatie) en het vastleggen van gegevens. De onderzoekshandelingen kunnen worden verricht met een technisch hulpmiddel.[3] Een technisch hulpmiddel in de zin van het Besluit onderzoek in een geautomatiseerd werk (hierna Besluit) is een 'softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel'.[4] Enigszins kort door de bocht houdt deze definitie het volgende in: een technisch hulpmiddel (meestal software) neemt gegevens waar (bijvoorbeeld een e-mail die op een telefoon van de verdachte staat) en verstuurt deze naar de politie.

De wet CCIII kent een aantal grondslagen om bij of krachtens Algemene Maatregel van Bestuur regels te stellen met betrekking tot de uitvoering van de bevoegdheid. In het Besluit zijn op basis van artikel 126ee Sv regels geformuleerd aangaande de onderzoekshandelingen die worden verricht met een technisch hulpmiddel. Deze regels moeten ertoe bijdragen dat de bevoegdheid niet wordt misbruikt en dat de authenticiteit en integriteit van de verkregen gegevens verzekerd kunnen worden.[5] Het Besluit bevat regels ten aanzien van de deskundigheid en autorisatie van opsporingsambtenaren, over de vastlegging van gegevens ter uitvoering van een bevel en ten aanzien van technische eisen die gesteld worden aan een technisch hulpmiddel en de keuring ervan. Verder zijn regels geformuleerd met betrekking tot het verrichten van onderzoekshandelingen in een geautomatiseerd werk en de verstrekking van tijdens het onderzoek verkregen gegevens.[6]

Zoals gezegd betreft één van de onderwerpen in het Besluit de keuring van technische hulpmiddelen.[7] Geregeld is dat een technisch hulpmiddel voorafgaand aan het gebruik ervan gekeurd wordt.[8] Hierop bestaan uitzonderingen.[9] In de toelichting op het Besluit

1 Artikel 80sexies Sr.
2 Het begrip geautomatiseerd werk is ruim gedefinieerd en kan betrekking hebben op veel verschillende apparaten. Ook een 'groep van onderling verbonden apparaten' wordt beschouwd als een geautomatiseerd werk (Van Uden & Van den Eeden, 2022).
3 Het gebruik van een technisch hulpmiddel is niet 'strikt noodzakelijk'. Soms zullen handelingen 'ad hoc en handmatig' worden verricht (Staatsblad 2018, 340, p. 16). Hierna wordt verwezen naar het Besluit onderzoek in een geautomatiseerd werk, 2018.
4 Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2.
5 *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54.
6 Besluit onderzoek in een geautomatiseerd werk, 2018, p. 13.
7 Hierop wordt uitgebreid ingegaan in de inleiding op de landenhoofdstukken.
8 Artikel 14 Besluit onderzoek in een geautomatiseerd werk.
9 Artikel 15 lid 1 en lid 2 Besluit onderzoek in een geautomatiseerd werk.

wordt duidelijk dat, indien de politie een technisch hulpmiddel wil gebruiken, dit in eerste instantie moet gebeuren met een technisch hulpmiddel dat gekeurd en goed bevonden is.[10] Na goedkeuring krijgt het technisch hulpmiddel een nummer toegekend dat gebruikt kan worden gedurende het opsporingsonderzoek en in het opsporingsdossier. Hierdoor hoeft de politie geen informatie prijs te geven over de samenstelling en werking van het middel. Daardoor worden opsporingsbelangen beschermd.[11] Sinds 2020 neemt de landelijke Keuringsdienst (onderdeel van de Dienst Specialistische Operaties (DSO) van de Nationale Politie) de keuringen voor haar rekening.

De Inspectie Justitie en Veiligheid houdt toezicht op de wijze waarop de politie uitvoering geeft aan de hackbevoegdheid. In haar eerste rapport in 2019 concludeert de Inspectie dat in geen van de zes zaken bij gebruikmaking van de hackbevoegdheid een vooraf goedgekeurd technisch hulpmiddel is ingezet. Daarnaast is in één zaak het technisch hulpmiddel achteraf ter keuring aangebonden. In de rest van de zaken is het technisch hulpmiddel niet ter keuring aangeboden.[12] In een Kamerbrief van de toenmalige Minister van Justitie en Veiligheid wordt aangegeven dat er een aantal oorzaken is waarom de keuring niet of maar beperkt plaatsvindt; dit zou onder meer komen door de beperkte ervaring met het ontwikkelen en inkopen van technische hulpmiddelen. Daarnaast blijkt uit het rapport van de Inspectie dat de keuring van commerciële middelen wordt bemoeilijkt, omdat de leverancier geen (volledige) inzage wil geven in zijn middel.[13] In zijn reactie geeft de minister ook aan dat de beslissing om een technisch hulpmiddel niet te laten keuren een 'uitzonderingsgeval' zou moeten zijn en niet 'lichtzinnig' moet worden genomen, omdat de betrouwbaarheid, integriteit en herleidbaarheid van de verzamelde gegevens 'cruciaal' zijn.[14] In zijn brief aan de Kamer zegt de minister toe dat een aanvullend onderzoek zal worden verricht naar de wijze waarop in (buiten-)landen waarmee Nederland intensief samenwerkt het gebruik van technische hulpmiddelen is georganiseerd. De uitkomsten kunnen als input dienen voor de bredere evaluatie van de wet CCIII[15] en vormen daarnaast een aanvulling op de al eerder verschenen evaluatie van de hackbevoegdheid in Nederland. Dit rapport is een verslag van het door de minister toegezegde aanvullende onderzoek.

1.2 Doelstelling en vraagstelling

De doelstelling van onderhavig onderzoek is om internationaal inzicht te krijgen in de wettelijke kaders die in verschillende landen bestaan voor de inzet van een hackbevoegdheid en voor de technische hulpmiddelen die daarbij (kunnen) worden toegepast. Indien er in landen geen (aparte) wet- en regelgeving bestaat voor de inzet van technische hulpmiddelen, is tevens het doel om te weten te komen of er andere waarborgen zijn die de betrouwbaarheid, herleidbaarheid en integriteit van de gegevens die verzameld worden met behulp van de hackbevoegdheid moeten garanderen.
De centrale onderzoeksvraag van dit onderzoek is als volgt:

[10] Besluit onderzoek in een geautomatiseerd werk, 2018.
[11] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 20.
[12] Inspectie JenV, 2020, p. 8-9. Ook uit de twee daarop volgende verslagen blijkt dat de meerderheid van de technische hulpmiddelen niet ter keuring wordt aangebonden. Wel is iets vaker gebruikgemaakt van een vooraf goedgekeurd technisch hulpmiddel en zijn meer technische hulpmiddelen ter keuring aangeboden (Inspectie JenV, 2021, p. 9; Inspectie JenV, 2022, p. 7).
[13] *Kamerstukken II* 2019/20, 29 628, nr. 970, p. 2-3. Dit komt ook naar voren in de WODC-evaluatie naar de uitvoering van de hackbevoegdheid in de praktijk (Van Uden & Van den Eeden, 2022).
[14] *Kamerstukken II* 2019/20, 29 628, nr. 970, p. 3.
[15] *Kamerstukken II* 2019/20, 29 628, nr. 970, p. 4.

Met welke waarborgen is in het buitenland de hackbevoegdheid, meer in het bijzonder het gebruik van technische hulpmiddelen omkleed en hoe verhoudt zich dat tot de Nederlandse situatie?

De centrale onderzoeksvraag wordt beantwoord aan de hand van de volgende deelvragen:

1 Welke landen kennen een 'hackbevoegdheid' en op basis van welke wettelijke grondslag kunnen buitenlandse politiediensten in hun eigen land gebruikmaken van de hackbevoegdheid?
2 Welke wettelijke voorwaarden gelden er in het buitenland voor politiediensten om de hackbevoegdheid in te kunnen zetten?
3 In hoeverre kennen andere landen een keuring van technische hulpmiddelen en wat is hierover in wet- en regelgeving vastgelegd?
4 In hoeverre gelden er nog andere regels om de betrouwbaarheid, herleidbaarheid en integriteit van de gegevens, die zijn verkregen met behulp van de inzet van technische hulpmiddelen, te waarborgen?
5 Hoe verhoudt de werkwijze in het buitenland zich tot de Nederlandse manier van werken met betrekking tot het keuren van technische hulpmiddelen en eventuele andere waarborgen om de betrouwbaarheid, integriteit en herleidbaarheid van gegevens te realiseren?

1.3 Methoden van onderzoek

1.3.1 Brede inventarisatie en selectie landen

Dit onderzoek betrof een internationaal vergelijkende studie. Voor het onderzoek is een brede inventarisatie gemaakt om in kaart te brengen welke landen een wettelijke hackbevoegdheid kennen. Om van een hackbevoegdheid te kunnen spreken hanteerden we als uitgangspunt dat de hackbevoegdheid heimelijk en op afstand plaatsvindt. In het kader van de brede inventarisatie zijn nagenoeg alle Europese landen bekeken plus de Verenigde Staten, Canada en Australië.[16] In de literatuur waren (verouderde) overzichten beschikbaar van landen die een hackbevoegdheid kennen.[17] De brede inventarisatie moest een actueel beeld geven welke landen over een wettelijke hackbevoegdheid beschikken en de wijze waarop in die landen de kwaliteit van gegevens gewaarborgd wordt.

Op basis van de brede inventarisatie is een selectie van vijf landen gemaakt die nader zijn bestudeerd.[18] De volgende criteria hebben een rol gespeeld bij de selectie: (1) de aanwezigheid van een hackbevoegdheid; (2) de aanwezigheid van een keuringsproces; (3) een instantie die een keuring of controle uitvoert van technische hulpmiddelen en (4) eventuele andere maatregelen die de kwaliteit van de gegevens moeten helpen waarborgen.[19] Tevens heeft een pragmatisch argument een rol gespeeld. Het bleek ingewikkeld, tijdrovend en soms ook niet mogelijk om in elk land dat in aanmerking

16 De VS, Canada en Australië zijn interessant omdat de Nederlandse politie samenwerkt met deze landen.
17 Zie onder meer: Eurojust (2016) & Gutheil, Liger, Heetman, Eager en Crawford (2017).
18 De brede inventarisatie en de verdiepende analyse van de vijf landen vonden deels parallel plaats. Dit in verband met de tijd die het kostte om een volledige brede inventarisatie te maken.
19 De minister zegt in zijn brief aan de Tweede Kamer expliciet toe onderzoek te doen naar de werkwijze in landen waarmee de Nederlandse politie intensief samenwerkt (*Kamerstukken II* 2019/20, 29 628, nr. 970, p. 4). Voor de selectie van landen hebben wij echter niet alleen dit criterium als uitgangspunt genomen. Een mogelijk risico van alleen het hanteren van dit selectiecriterium was dat mogelijk interessante landen gemist zouden worden die bijvoorbeeld een keuringsproces hebben ingericht of gebruikmaken van andere maatregelen om de betrouwbaarheid, integriteit en herleidbaarheid van gegevens te waarborgen.

kwam voor de selectie voldoende contacten te leggen. Om die reden zijn Spanje, Denemarken en het Verenigd Koninkrijk afgevallen. In tabel 1.1 is te zien welke landen meer diepgaand konden worden bestudeerd, inclusief een motivatie het betreffende land te selecteren.

Tabel 1.1 Motivatie selectie landen

Land	Motivatie
België	Kent een wettelijke hackbevoegdheid.
	In de wet wordt gesproken over 'passende middelen' in verband met de vertrouwelijkheid en integriteit van gegevens.
Duitsland	Kent een wettelijke hackbevoegdheid.
	Aanwezigheid van een instantie (ZITiS) die zich bezighoudt met het ontwikkelen en onderzoeken van technische hulpmiddelen.
	Verschillende waarborgen aanwezig ten aanzien van het gebruik van digitale gegevens.
Frankrijk	Kent een wettelijke hackbevoegdheid.
	Aanwezigheid van een instantie (STNCJ) die de kwaliteit van de gebruikte technische hulpmiddelen bewaakt.
Zweden	Kent een wettelijke hackbevoegdheid.
	Aanwezigheid van een instantie (SIN) die de kwaliteit van de inzet van de hackbevoegdheid monitort.
Zwitserland	Kent een wettelijke hackbevoegdheid.
	In de wet worden eisen gesteld aan de technische hulpmiddelen die gebruikt worden, zoals logging en het prijsgeven van de broncode.

1.3.2 Onderzoeksmethoden

Om de onderzoeksvragen te beantwoorden zijn verschillende onderzoeksmethoden gebruikt: documentstudie (wet- en regelgeving en relevante (grijze) literatuur), schriftelijke vragenlijsten en interviews. In bijlage 1 staat per land weergegeven welke bronnen geraadpleegd zijn. In onderstaande tekst worden de onderzoeksmethoden nader toegelicht.

Wet- en regelgeving en literatuurstudie
Voor dit onderzoek is bestaande wet- en regelgeving bestudeerd. Daarnaast is literatuur geanalyseerd die de wet- en regelgeving bespreekt. Daarbij is gebruikgemaakt van zowel grijze literatuur als wetenschappelijke artikelen, te vinden via Google (Scholar) en digitale bibliotheken die geraadpleegd konden worden via het Rijksportaal. Soms zijn ook krantenberichten geraadpleegd, bijvoorbeeld omdat daarin gesproken werd over technische hulpmiddelen waarvan de politie in dat land gebruik zou maken. Relevante documentatie werd niet alleen gevonden via zoekmachines, maar ook via geïnterviewden die wij spraken (zie later). Vervolgens werd op basis van de sneeuwbalmethode aanvullende literatuur gezocht en bestudeerd (Boeije, 2008). We probeerden zoveel mogelijk Engelstalige documenten te raadplegen. Indien dat niet mogelijk bleek, hebben we gebruikgemaakt van Google Translate, waarmee het betreffende document werd omgezet naar het Engels. Een enkele keer raadpleegden

wij een *native speaker* die ons van een vertaling voorzag. Naast de literatuur en wet- en regelgeving is ook gezocht naar beschikbare jurisprudentie. Hierbij lag de nadruk op beschikbare jurisprudentie waarin de kwaliteit van gegevens verkregen met de hackbevoegdheid centraal stond. Vanwege het grote aantal landen in dit onderzoek was het niet mogelijk om in ieder land een jurisprudentieonderzoek uit te voeren. In plaats daarvan hebben wij gebruikgemaakt van de respondenten in dit onderzoek en hun de vraag voorgelegd of er relevante jurisprudentie is. Onze inventarisatie van relevante jurisprudentie is daarmee niet uitputtend.

Mailing experts

Ten behoeve van de *brede inventarisatie* is via Eurojust (the *European Union Agency for Criminal Justice Cooperation*) een korte vragenlijst uitgezet. Eurojust brengt binnen Europa officieren van justitie en rechters samen om grensoverschrijdende vormen van criminaliteit tegen te gaan (Eurojust, z.d.). Verder is Eurojust een belangrijke partner van het European Judicial Cybercrime Network (ECJN), een netwerk dat als doel heeft de samenwerking tussen judiciële autoriteiten op het gebied van cybercrime, gedigitaliseerde criminaliteit en digitale opsporing te verbeteren (Eurojust, z.d.). Aan de Europese lidstaten zijn, door tussenkomt van Eurojust, vier vragen voorgelegd over de volgende onderwerpen: de aanwezigheid van een (wettelijke) hackbevoegdheid, relevante wet- en regelgeving en literatuur, de aanwezigheid van een keuring van technische hulpmiddelen en eventuele andere maatregelen die genomen moeten worden in het kader van de kwaliteit van gegevens. De vragenlijst is door 14 van de 26 landen ingevuld. Een mogelijke verklaring voor het feit dat niet alle landen een vragenlijst hebben ingevuld is dat de vragenlijst geen onderdeel was van een verplicht in te vullen 'questionnaire'. In zo'n geval zijn landen binnen Eurojust verplicht om te antwoorden.

Interviews

Ten behoeve van de brede inventarisatie hebben verkennende interviews plaatsgevonden met wetenschappers die zich bezighouden met cybergerelateerde onderwerpen en de inzet van (nieuwe) opsporingsbevoegdheden. De interviews vonden plaats gedurende de periode februari 2022 en december 2022. Soms benaderden we hen naar aanleiding van een concrete publicatie, andere keren kwamen we hen op het spoor via een algemeen e-mailadres van een faculteit die zich met een voor ons relevant onderwerp bezighield. We hielden ook een aantal verkennende interviews met personen die in de praktijk te maken hebben met cybergerelateerde zaken zoals een officier van justitie, een politieagent of een advocaat.[20] Dat gebeurde doorgaans wanneer deze personen ons gesuggereerd werden door de wetenschappers die wij benaderden of wanneer we geen antwoorden kregen via de korte vragenlijst uitgezet bij Eurojust. Ook hadden we soms aanvullende vragen naar aanleiding van de korte Eurojust-vragenlijst. Uiteindelijk hebben we twintig verkennende interviews met tweeëntwintig personen afgenomen. De meeste interviews hadden betrekking op één land, in enkele gevallen werden twee of drie landen besproken. Het kwam ook voor dat het niet mogelijk was om een verkennend interview te houden, bijvoorbeeld vanwege drukke agenda's van de mogelijk te interviewen personen of omdat zij de voorkeur gaven aan een vragenlijst per e-mail. In die gevallen hebben wij per e-mail een aantal vragen gesteld die relevant waren voor de brede inventarisatie. We hebben negen aanvullende vragenlijsten via de mail verstuurd.

[20] Het onderscheid tussen wetenschapper en uitvoeringsprofessional was overigens niet altijd helder, omdat iemand soms zowel wetenschapper was als uitvoeringsprofessional, bijvoorbeeld een advocaat.

Tijdens de verkennende interviews (en vragenlijsten via de mail) stelden we onder andere vragen over de aanwezigheid van de hackbevoegdheid, het gebruik van technische hulpmiddelen, maatregelen in het kader van de kwaliteit van te verzamelen/verzamelde gegevens en mogelijke rechtszaken die er waren geweest.

Naast de zojuist besproken verkennende interviews hielden we verdiepende interviews met personen in de door ons geselecteerde vijf landen. Het doel van deze verdiepende interviews was het krijgen van een volledi ger beeld op welke manier de wettelijke hackbevoegdheid in dat land geregeld was. Via eerdere contacten (de sneeuwbal-methode) werden deze personen benaderd. Per land spraken we in principe met een vertegenwoordiger van het ministerie dat zich bezighield met wetgeving op het terrein van opsporingsbevoegdheden, meer in het bijzonder hacken, en met vertegenwoordigers van het Openbaar Ministerie, van de politie en van een instantie die betrokken was bij het toezicht op de bevoegdheid/het gebruik van technische hulpmiddelen.[21] Ook voor deze interviews gold dat we ons soms beperkt hebben tot een vragenlijst via e-mail, onder meer omdat de betreffende persoon of organisatie daar, vanwege de vertrouwelijke aard van de materie, de voorkeur aangaf. Een enkele keer wilden één van deze functionarissen ons niet te woord staan of geen vragen via de e-mail beantwoorden. In totaal hielden we veertien verdiepende interviews en verstuurden we drie verdiepende vragenlijsten. Tijdens de interviews stelden we onderwerpen aan de orde die ook naar voren kwamen tijdens de verkennende interviews. Daarnaast voegden we vragen toe die toegespitst waren op de betreffende functie van de geïnterviewde. Ook voegden we vragen toe over onderwerpen die op basis van eerdere interviews en de analyse van relevante documenten onvoldoende duidelijk waren geworden.

Om de vertrouwelijkheid van de geïnterviewden te borgen worden zij in dit onderzoek niet met naam en toenaam genoemd. Naar informatie afkomstig uit interviews wordt verwezen middels ´persoonlijke communicatie´. Dat gebeurt ook bij passages die zijn toegevoegd op basis van antwoorden op de door de onderzoekers gestelde aanvullende vragen en eventuele correcties die individuele aangaven ten aanzien van de door ons opgestelde teksten.

Beperkingen

De gekozen onderzoeksmethoden kennen een aantal beperkingen. Ten eerste richten wij ons in het onderzoek op de wettelijk vastgelegde vereisten. Hierdoor vielen (informele) beleidsregels, die bijvoorbeeld de politie hanteert ten aanzien van de omgang met verkregen gegevens, buiten de scope van het onderzoek. Waar beschikbaar hebben we informatie over de beleidsregels wel opgenomen, maar in de meeste gevallen bleken de beleidsregels, voor zover aanwezig, vertrouwelijk en niet openbaar beschikbaar. Dit onderzoek is dus vooral een weergave van de wettelijke regelingen die in de verschillende landen bestaan. Ten tweede verwijzen wij in het rapport naar beschikbare jurisprudentie. Wij hebben, onder andere vanwege beperkingen in de tijd, geen volledig jurisprudentieonderzoek uitgevoerd. In plaats daarvan baseren wij ons op beschikbare literatuur en interviews. De inventarisatie is daarom niet uitputtend en dit onderzoek geeft een eerste beeld van jurisprudentie die al dan niet aanwezig is. Ten derde lag het zwaartepunt van de dataverzameling bij het houden van interviews. Voor de landen die uitgebreider zijn geanalyseerd (zie tabel 1.1) is geprobeerd in ieder

[21] Het was van te voren niet altijd duidelijk of een persoon bij het Openbaar Ministerie werkte of bij het ministerie. In Frankrijk bijvoorbeeld is het gebruikelijk dat men een aantal jaren als officier van justitie werkt, en vervolgens een aantal jaar op het ministerie. Om die reden hebben we in Frankrijk twee personen gesproken van het ministerie en géén vertegenwoordiger van het Openbaar Ministerie.

land met de politie, het Openbaar Ministerie, de wetgever (betrokken ministerie) en een wetenschapper te spreken. Het streven daarbij was om een zo compleet mogelijk beeld te krijgen van de hackbevoegdheid in deze landen. Het is echter niet in alle landen gelukt om met al deze partijen te spreken. De belangrijkste oorzaken waren dat respondenten in sommige gevallen niet mee wilden werken vanwege de gevoelige aard van de materie en in andere gevallen kregen wij na meerdere pogingen geen reactie. Desondanks waren wij toch goed in staat de onderzoekvragen te beantwoorden. Ten slotte richten wij ons in dit onderzoek op het heimelijk op afstand hacken van geautomatiseerde werken. Daarmee valt het fysiek hacken van apparaten buiten de scope van dit onderzoek.

1.4 Analyse

Op het moment dat een belangrijk deel van de data verzameld was, zijn we gestart met de analyse. Tussentijds vonden ook al eerste analyses plaats om de juiste vragen te kunnen stellen tijdens de verdiepende interviews. Voor de hoofdanalyse is in *Word* een lijst met codes opgesteld. Deze codes waren gebaseerd op de belangrijkste onderdelen voortkomend uit de onderzoeksvragen. Voorbeelden van codes waren wettelijke grondslag, onderzoekshandelingen, keuring of andere maatregelen om de kwaliteit van gegevens te kunnen waarborgen. Ook wettelijke voorwaarden zoals type misdrijven en de periode waarbinnen de bevoegdheid mocht worden ingezet, stonden op de codelijst. Voor alle landen is een codelijst ingevuld. Dit werk werd verdeeld onder de drie onderzoekers. Daarbij bestond ook de mogelijkheid om zelf nog codes toe te voegen, indien die relevant bleken voor het betreffende land. Vanwege de omvang van de informatie maakten we geen gebruik van een analyseprogramma zoals bijvoorbeeld Maxqda, maar heeft de analyse handmatig plaatsgevonden.

Op basis van de codelijsten per land is een algemeen overzicht gemaakt van de verschillende landen (hoofdstuk 2) en zijn de vijf geselecteerde landen meer diepgaand beschreven (hoofdstuk 3 tot en met 7). De landentabellen en individuele landenhoofdstukken zijn ter controle op feitelijke onjuistheden voorgelegd aan de contactpersonen uit de verschillende landen.

1.5 Opbouw van het rapport

Dit rapport is als volgt opgebouwd. In hoofdstuk 2 volgt een landenoverzicht. Eerst wordt met behulp van een landkaart aangegeven welke landen een hackbevoegdheid kennen. Ook wordt op hoofdlijnen een beschrijving gegeven van de aanwezige wettelijke voorwaarden. Het tweede deel van dat hoofdstuk bevat een aantal overzichtstabellen met daarin de waarborgen die de verschillende landen kennen ten aanzien van het bevorderen van de kwaliteit van de verzamelde gegevens. Hoofdstukken 3 tot en met 7 bevatten uitgebreide beschrijvingen van de door ons geselecteerde landen. Respectievelijk België, Duitsland, Frankrijk, Zweden en Zwitserland komen aan bod. In hoofdstuk 8 richt de aandacht zich op de conclusie. Daarin worden de door ons geselecteerde landen onderling vergeleken. Ook wordt een vergelijking gemaakt met Nederland. Het einde van dit hoofdstuk bevat een aantal scenario's.

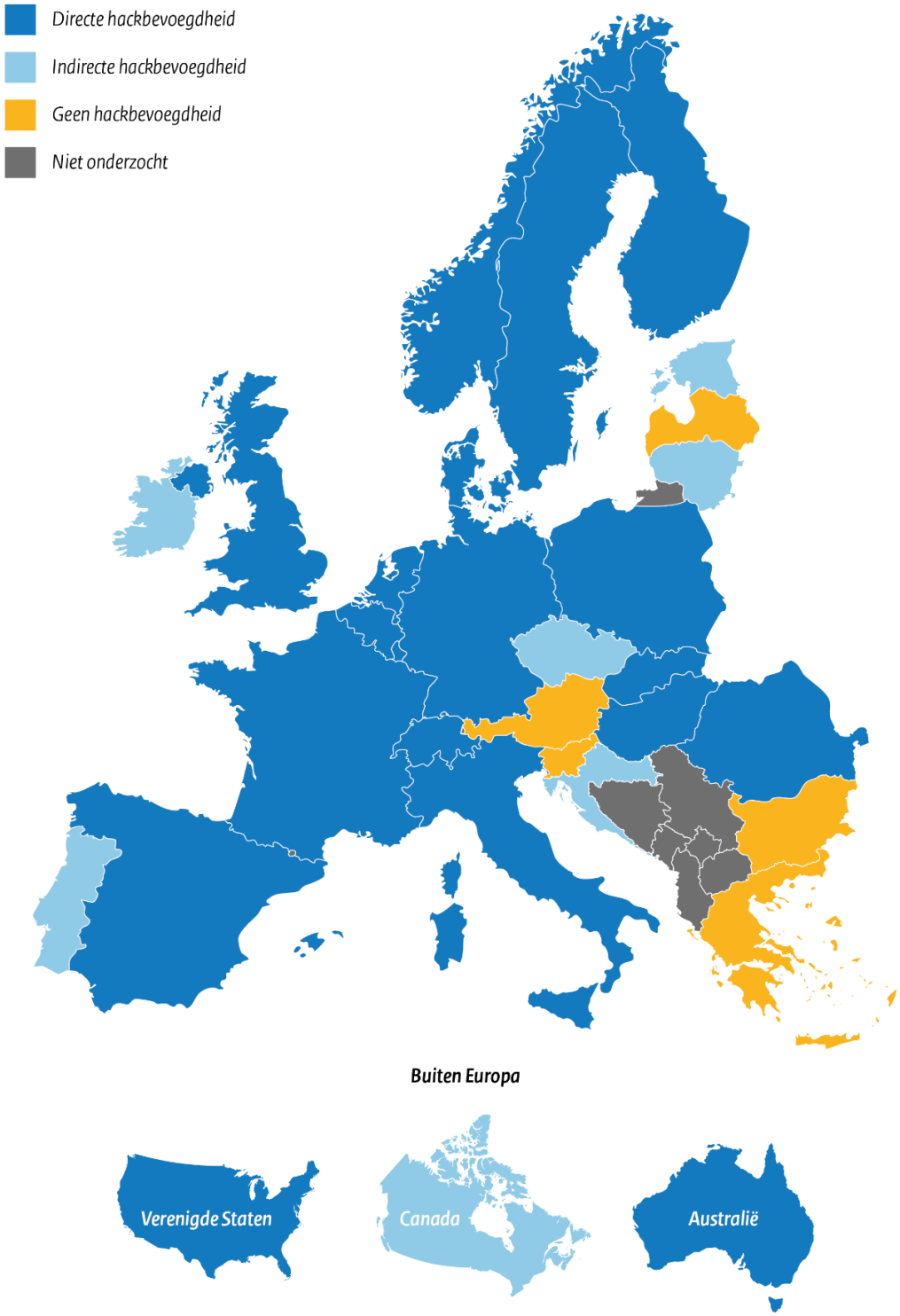
2 Landenoverzicht

In dit hoofdstuk wordt met betrekking tot een groot aantal Europese landen en Australië, Canada en de Verenigde Staten een overzicht gegeven van de aanwezigheid van een hackbevoegdheid. Paragraaf 2.1 richt zich op de vraag of een land een hackbevoegdheid kent inclusief de voorwaarden die gelden om de bevoegdheid in te mogen zetten en de onderzoekshandelingen die kunnen worden verricht. Deze paragraaf start met een figuur waarin in één oogopslag te zien is welke landen een hackbevoegdheid kennen. Vervolgens wordt op hoofdlijnen een aantal voorwaarden besproken. In paragraaf 2.2 worden vervolgens de waarborgen uiteengezet die in de verschillende landen ervoor moeten zorgen dat de kwaliteit van de verzamelde gegevens op orde is. Hoewel in dit hoofdstuk nog geen vergelijking met Nederland wordt gemaakt, is Nederland ter informatie in de verschillende tabellen opgenomen.

2.1 Aanwezigheid hackbevoegdheid en voorwaarden

Figuur 2.1 bevat een kaart van alle landen die zijn opgenomen in dit onderzoek. Het figuur geeft weer of het land een wettelijke hackbevoegdheid voor de politie kent en zo ja, of dit een directe of indirecte bevoegdheid is. Van een directe bevoegdheid is sprake als de wet expliciet de mogelijkheid noemt om een geautomatiseerd werk heimelijk en op afstand binnen te dringen en daarbinnen één of meerdere onderzoeks-handelingen te verrichten. Van een indirecte bevoegdheid is sprake als de hack-bevoegdheid deel uitmaakt van een algemene bepaling. Dit gaat bijvoorbeeld om een interceptiebevoegdheid, waarbij in de wetstekst niet specifiek de hackbevoegdheid wordt genoemd, maar de bevoegdheid wel voor dat doel wordt ingezet.

Figuur 2.1 Landenoverzicht hackbevoegdheid



Kaarten zijn bewerkingen van werken van Maix (Europa; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; publiek domein) en Rycherr (Australië; CC BY-SA 4.0 en eerdere versies).

Met behulp van de hackbevoegdheid mag de politie in de verschillende landen diverse onderzoekshandelingen verrichten. In bijlage 2 worden deze handelingen voor de verschillende landen nader gespecificeerd. In tabel 2.1 staan de drie meest voorkomende onderzoekshandelingen weergegeven. Hierbij gaat het om (1) het doorzoeken en opslaan van gegevens van het geautomatiseerd werk; (2) interceptie van communicatie (audio, beeld, internetverkeer); en (3) surveillance-activiteiten zoals het activeren van de microfoon, camera of GPS op het geautomatiseerd werk. Daarnaast is aangegeven als de wet niet specificeert welke handelingen wel of niet mogen worden verricht bij de inzet van de hackbevoegdheid.

Tabel 2.1 Onderzoekshandelingen hackbevoegdheid

Land	Doorzoeken	Interceptie	Surveillance	Geen vereisten
Australië	X			
België				X
*Bulgarije**				
Canada				X
Denemarken				X
Duitsland	X	X		
Estland				X
Finland	X	X		
Frankrijk	X	X		
*Griekenland**				
Hongarije	X	X		
Ierland	X		X	
Italië		X	X	
Kroatië	X	X	X	
*Letland**				
Litouwen				X
Luxemburg		X		
Nederland	X	X	X	
Noorwegen	X	X	X	
*Oostenrijk**				
Polen	X	X	X	
Portugal	X	X	X	
Roemenië	X	X	X	
*Slovenië**				
Slowakije	X	X	X	
Spanje				X
Tsjechië				X
Verenigd Koninkrijk	X	X	X	
Verenigde Staten	X			
Zweden	X	X	X	
Zwitserland		X		

* Geen hackbevoegdheid.

Voor de helft van de landen geldt dat alle drie de onderzoekshandelingen mogen worden ingezet. In zeven landen zijn geen vereisten opgenomen wat betreft de onderzoekshandelingen. Dat betekent dat in principe iedere handeling kan worden opgenomen in het bevel en het aan de rechter is om te beoordelen of daar ook een machtiging voor kan worden afgegeven. Tenslotte is bij de landeninventarisatie gekeken of er jurisprudentie beschikbaar is (niet op basis van een volledige jurisprudentieanalyse) waarin de kwaliteit van gegevens verkregen met de hack-bevoegdheid ter discussie is gesteld. Opvallend is dat – voor zover ons bekend – maar in twee landen (Frankrijk en Zweden) jurisprudentie te vinden is waarin de kwaliteit van de gegevens bediscussieerd is. Een mogelijke conclusie zou kunnen zijn dat de kwaliteit van de gegevens niet ter discussie wordt gesteld. Het is echter niet uit te sluiten dat deze discussie wel plaatsvindt, maar niet terecht komt in de rechterlijke uitspraak waardoor deze discussie niet zichtbaar is. Geïnterviewden geven op basis van eigen ervaring aan weinig zaken te kennen waarin de kwaliteit van de gegevens ter discussie is gesteld. Dit zou volgens hen onder meer kunnen komen door een gebrek aan technische kennis bij de verdediging en/of het aanvullende (overtuigend) bewijs dat gepresenteerd wordt. Mogelijk dat toekomstige jurisprudentie leidt tot aanpassingen van wetgeving, zoals het aanscherpen van de waarborgen ten aanzien van de kwaliteit van de verzamelde gegevens. Een dergelijke situatie deed zich voor in Frankrijk waar mogelijk als aanvullende waarborg een certificaat van echtheid moet worden afgegeven door de dienst die de bevoegdheid uitvoert en de gegevens veiligstelt (zie voor een uitgebreidere bespreking paragraaf 5.9).[22]

2.2 Waarborgen ten aanzien van de verzamelde gegevens

In deze paragraaf wordt ingegaan op de wettelijke waarborgen die gelden ten aanzien van gegevens die worden verzameld met behulp van de hackbevoegdheid. Het betreft hier in beginsel waarborgen die specifiek staan genoemd in het wetsartikel waarin de hackbevoegdheid is geregeld of die in andere wetsartikelen worden genoemd die samenhangen met het wetsartikel op basis waarvan de politie de hackbevoegdheid mag inzetten. Waar mogelijk komen informele waarborgen aan bod, bijvoorbeeld afkomstig uit interne beleidsregels of *best practices* die de politie hanteert. Omdat deze waarborgen een informeel karakter hebben en lang niet altijd formeel zijn vastgelegd en/of wij er tijdens ons onderzoek geen goed beeld van hebben kunnen krijgen, ligt de focus in dit rapport op de waarborgen die wettelijk geregeld zijn.

In de inventarisatie zijn de volgende categorieën van waarborgen naar voren gekomen:

- Aanwezigheid van een keuring van technische hulpmiddelen door een onafhankelijke instantie.
- Aanwezigheid van een onafhankelijke instantie die zich specifiek bezighoudt met een controle op de inzet van de hackbevoegdheid. (Algemene) toezichthouders, die zich bijvoorbeeld richten op het toezicht op de gehele politietaak, zijn buiten beschouwing gelaten.
- Regels ten aanzien van het documenteren en loggen van uitgevoerde onderzoekshandelingen zodat uitgevoerde handelingen transparant en herleidbaar zijn.
- Aanwezigheid van rechterlijk toezicht. Hierbij gaat het niet om de vraag of voorafgaande toestemming nodig is van een (onderzoeks)rechter, maar om de

[22] Hof van Cassatie, strafkamer, 11 oktober 2022, beroep nr. 21-85.148.

vraag of gedurende de inzet een (onderzoeks)rechter toezicht houdt op de uitvoering van de bevoegdheid.
- Regels ten aanzien van de opslag van gegevens verkregen met behulp van de hackbevoegdheid.
- Voorwaarden die gelden als een zaak ter zitting komt en de wijze waarop het inzagerecht voor de verdachte is vormgegeven.

In onderstaande tekst wordt ingegaan op de belangrijkste bevindingen die naar voren zijn gekomen in de inventarisatie. In de komende (samenvattende) tabellen zijn alleen de landen opgenomen die daadwerkelijk een hackbevoegdheid kennen. Bijlage 3 bevat een uitgebreidere tabel met daarin een overzicht van de waarborgen die de verschillende landen hanteren ten aanzien van de gegevens die worden verzameld met behulp van de hackbevoegdheid.[23]

2.2.1 Keuring technische hulpmiddelen en controlerende instantie

Tabel 2.2 Aanwezigheid keuring en controlerende instantie

Land	Keuring	Controlerende instantie
Australië	Nee	Ombudsman
België	Nee	Nee
Canada	Nee	Nee
Denemarken	Nee	Deense Onafhankelijke Raad voor toezicht op bewijsmateriaal
Duitsland	Nee	Het Centraal Bureau voor Informatietechnologie in de Beveiligingssector (ZITiS)
Estland	Nee	Nee
Finland	Nee	Nee
Frankrijk	Nee	Service technique national de captation judiciaire (STNCJ)
Hongarije	Nee	Nee
Ierland	Nee	Nee
Italië	Nee	Nee
Kroatië	Nee	Nee
Litouwen	Nee	Nee
Luxemburg	Nee	Nee
Nederland	Ja	Keuringsdienst
Noorwegen	Nee	Controlecomité dwangmiddelen
Polen	Nee	Nee
Portugal	Nee	Nee
Roemenië	Nee	Nee
Slowakije	Nee	Nee
Spanje	Nee	Nee

[23] Bijlage 1 bevat een overzicht van de verschillende bronnen die zijn geraadpleegd voor de informatie in het overzicht.

Land	Keuring	Controlerende instantie
Tsjechië	Nee	Nee
Verenigd Koninkrijk	Nee	Investigatory Powers Commissioner's Office (IPCO) & Investigatory Powers Tribunal
Verenigde Staten	Nee	Nee
Zweden	Nee	Commissie voor Veiligheid en Integriteitsbescherming (SIN)
Zwitserland	Nee	Nee

Geen enkel land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keurings-protocol, de technische hulpmiddelen dient te onderzoeken. Sommige landen kennen wel een testprocedure, maar dit wordt niet uitgevoerd door een onafhankelijke keuringsdienst. Verder geldt voor de overige landen die een keuring of testprocedure kennen dat onbekend is hoe de procedure eruitziet. Duitsland vormt hierop een uitzondering. Ook daar is niet volledig duidelijk hoe de keuring eruitziet, maar het is wel bekend dat deze gebaseerd is op een speciaal daarvoor geformuleerde SLB-richtlijn (zie paragraaf 4.8).

Het toezicht op de uitvoering van de bevoegdheid door een onafhankelijke instantie is in het buitenland beperkt (de zittingsrechter buiten beschouwing gelaten). Voor Australië, Denemarken, Noorwegen, het Verenigd Koninkrijk en Zweden geldt dat een vorm van toezicht plaatsvindt op de uitvoering van de bevoegdheid door een onafhankelijke instantie. Daarnaast bestaat in Duitsland een instantie die, vanwege haar technische expertise, adviseert over de inzet en ontwikkeling van technische hulpmiddelen. Frankrijk kent een specifieke instantie die verantwoordelijk is voor het ontwerp, de aansturing en de implementatie van technische hulpmiddelen die gebruikt worden voor de hackbevoegdheid. Op de instanties in Zweden, Duitsland en Frankrijk wordt in de komende hoofdstukken nader ingegaan.

2.2.2 *Documentatie, opslag en rechterlijk toezicht*

Tabel 2.3 Waarborgen voor documentatie, opslag en rechterlijk toezicht

Land	Waarborgen voor documenteren handelingen	Rechterlijk toezicht gedurende inzet	Waarborgen voor opslag gegevens
Australië	Ja	Nee	Ja
België	Ja	Ja	Ja
Canada	Ja	Nee	Nee
Denemarken	Onbekend	Nee	Nee
Duitsland	Ja	Nee	Ja
Estland	Ja	Nee	Nee
Finland	Onbekend	Nee	Ja
Frankrijk	Ja	Ja	Ja
Hongarije	Ja	Nee	Ja
Ierland	Onbekend	Nee	Nee
Italië	Ja	Nee	Ja
Kroatië	Ja	Ja	Ja
Litouwen	Ja	Nee	Nee
Luxemburg	Ja	Nee	Ja
Nederland	Ja	Nee	Ja
Noorwegen	Ja	Nee	Ja
Polen	Ja	Nee	Ja
Portugal	Ja	Ja	Ja
Roemenië	Ja	Nee	Ja
Slowakije	Ja	Nee	Ja
Spanje	Ja	Ja	Ja
Tsjechië	Ja	Nee	Ja
Verenigd Koninkrijk	Ja	Nee	Ja
Verenigde Staten	Ja	Nee	Ja
Zweden	Onbekend	Nee	Nee
Zwitserland	Ja	Nee	Ja

Ten aanzien van het documenteren en loggen van uitvoeringshandelingen geldt dat in vrijwel alle landen een vorm van documentatie vereist is. Dit betekent dat op zijn minst een proces-verbaal moet zijn opgesteld waarin alle handelingen staan gedocumenteerd. Sommige landen gaan een stap verder, omdat daar alle handelingen moeten worden gelogd. Voor vijf landen is gedurende ons onderzoek niet duidelijk geworden of daar eisen worden gesteld aan het documenteren en loggen van uitvoeringshandelingen.

In België, Frankrijk, Kroatië, Portugal en Spanje vindt *gedurende* de inzet van de bevoegdheid rechterlijk toezicht plaats. Dit betekent dat de politie tussentijds aan de rechter die de machtiging heeft verleend, statusupdates moet geven over de voortgang. In sommige gevallen kan de rechter op basis daarvan besluiten de toestemming voor de inzet van de bevoegdheid in te trekken. Voor de overige landen geldt dat – voor zover bekend – geen tussentijds rechterlijk toezicht plaatsvindt.
Twintig landen kennen in de wet opgenomen waarborgen ten aanzien van de opslag van gegevens die zijn verkregen met de hackbevoegdheid. Hierbij gaat het onder meer om het verzegeld opslaan van de gegevens of het opslaan van de gegevens in een beveiligde omgeving. Voor de overige landen geldt dat er niets is opgenomen in de wet of dat ons niet duidelijk is geworden of landen (informele) waarborgen kennen.

2.2.3 Zitting en inzagerecht

Tabel 2.4 Notificatieplicht en inzagerecht

Land	Notificatieplicht	Inzagerecht
Australië	Nee	Nee
België	Ja	Ja
Canada	Ja	Ja
Denemarken	Ja	Ja
Duitsland	Ja	Nee
Estland	Ja	Ja
Finland	Nee	Nee
Frankrijk	Nee, alleen bij aanvang rechtszaak	Ja
Hongarije	Nee	Nee
Ierland	Nee, tenzij verplicht door rechter	Nee
Italië	Nee	Ja
Kroatië	Ja	Ja
Litouwen	Ja, tenzij opsporingsbelang wordt geschaad	Ja
Luxemburg	Nee, alleen bij aanvang rechtszaak	Ja
Nederland	Ja	Ja
Noorwegen	Ja, tenzij staatsgeheim	Ja
Polen	Nee	Nee
Portugal	Ja	Nee, alleen als het openbaar is
Roemenië	Nee	Ja
Slowakije	Nee	Ja
Spanje	Nee	Ja
Tsjechië	Ja	Ja
Verenigd Koninkrijk	Nee	Nee
Verenigde Staten	Nee	Ja

Land	Notificatieplicht	Inzagerecht
Zweden	Ja, tenzij opsporingsbelang wordt geschaad	Ja
Zwitserland	Ja	Nee

In dertien landen is een notificatieplicht opgenomen in de wet. Dat betekent dat personen van wie het geautomatiseerd werk is binnengedrongen binnen een bepaalde termijn geïnformeerd moeten worden dat de bevoegdheid is ingezet. In de helft van deze landen kan notificatie worden uitgesteld of soms zelfs achterwege blijven als opsporingsbelangen in het gedrang kunnen komen. Voor vrijwel alle landen geldt dat de verdachte wordt genotificeerd, als een zaak ter zitting komt. Verder is in zeventien landen het recht op inzage tot de verkregen gegevens expliciet opgenomen in de wet. In veel gevallen kan de verdediging een kopie van de verkregen gegevens ontvangen. Bij de overige landen is in onze inventarisatie niet naar voren gekomen of voor de bevoegdheid een specifieke wettelijke bepaling is opgenomen ten aanzien van het recht op inzage.

Inleiding op de landenhoofdstukken

In de komende hoofdstukken volgt een beschrijving van de door ons geselecteerde landen.[24] Achtereenvolgens bespreken we België, Duitsland, Frankrijk, Zweden en Zwitserland. Per land geven we een beschrijving hoe de hackbevoegdheid geregeld is. Daarbij wordt grotendeels de indeling van Corstens en collega's (2018) gevolgd. Dat betekent dat we per land de volgende onderwerpen bespreken: een uiteenzetting van de wijze waarop de hackbevoegdheid gedefinieerd is, de bevoegde autoriteiten en het daarbij behorende proces. Ook wordt aandacht besteed aan de personen en de geautomatiseerde werken tegen wie/waartegen de bevoegdheid mag worden ingezet. Daarna richt de aandacht zich op het soort misdrijven (de gevallen), de termijn en de formaliteiten. Vervolgens besteden we aandacht aan de technische hulpmiddelen die mogen worden gebruikt en de waarborgen die gelden, vooral ten aanzien van de kwaliteit van de verzamelde gegevens. We besluiten steeds met de beschikbare jurisprudentie en een korte slotbeschouwing.

Om uiteindelijk een vergelijking te kunnen maken tussen de zojuist genoemde landen en Nederland wordt in deze inleiding eerst een beschrijving gegeven van de Nederlandse situatie. Dit betreft een zeer summiere beschrijving van het wettelijk kader. Daarnaast wordt ingegaan op de verschillende waarborgen die Nederland kent om de kwaliteit van de verzamelde gegevens te waarborgen. Daarbij wordt ook stilgestaan bij de uitvoeringspraktijk. Dat laatste is van belang om op zinvolle wijze een vergelijking tussen Nederland en het buitenland te kunnen maken (zie hoofdstuk 8). Een uitgebreide beschrijving van de Nederlandse situatie is te vinden in een eerder verschenen WODC-rapport (Van Uden & Van den Eeden, 2022) en in bijlage 4 van dit rapport. De informatie beschreven in dit hoofdstuk is gebaseerd op bevindingen uit het eerder verschenen WODC-rapport (Van Uden & Van den Eeden, 2022).

Hackbevoegdheid in Nederland

Sinds 1 maart 2019 beschikt de Nationale politie in Nederland over een hackbevoegdheid. Dat betekent dat een specialistisch team – onder bepaalde voorwaarden – geautomatiseerde werken in gebruik van verdachten, zoals telefoons en servers, heimelijk en op afstand kan binnendringen en gegevens kan verzamelen. De politie mag een aantal onderzoekshandelingen verrichten om gegevens te verzamelen, welke staan opgesomd in artikel 126nba lid 1 Sv. Bij de (uitvoering van de) bevoegdheid zijn zowel technische als tactische actoren betrokken. Vanuit de technische kant is dat Digit (*Digital Intrusion Team*). Digit zelf kent twee onderdelen: Digit-politie en Digit-OM. De uitvoering van de hackbevoegdheid is in handen van Digit-politie, onderdeel van de Landelijke Eenheid van de Nationale Politie. Digit-politie wordt aangestuurd door Digit-OM dat ondergebracht is bij het Landelijk Parket van het Openbaar Ministerie. Een inzet van de hackbevoegdheid door Digit (hierna 'inzet') vindt plaats binnen een al lopend opsporingsonderzoek. Dat opsporingsonderzoek wordt uitgevoerd door een tactisch team van de politie (bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime) onder gezag van een zaaksofficier van justitie. Deze zaaksofficier is eindverantwoordelijk voor het opsporingsonderzoek waarbinnen Digit een

[24] Zie voor een toelichting op de geselecteerde landen, hoofdstuk 1.

inzet doet en hij/zij dient verantwoording af te leggen in de rechtbank als een zittingsrechter de zaak behandelt.

Voor het verrichten van onderzoekshandelingen kan de politie een technisch hulpmiddel gebruiken. In principe dient de Nederlandse politie gebruik te maken van een technisch hulpmiddel dat voorafgaand aan het gebruik ervan gekeurd en goed bevonden is door de Keuringsdienst. In Nederland bestaat gedetailleerde regelgeving met betrekking tot maatregelen die de kwaliteit van de verzamelde gegevens moet waarborgen. Een belangrijk deel hiervan is opgenomen in het Besluit.[25] Maatregelen hebben vooral betrekking op de periode voorafgaand aan de inzet, maar ook ten aanzien van de periode tijdens en na een inzet van de hackbevoegdheid kunnen waarborgen worden onderscheiden.

Waarborgen voorafgaand aan de inzet

Wat betreft de periode voorafgaand aan de inzet, zijn in het Besluit diverse regels opgenomen waaraan een technisch hulpmiddel moet voldoen. Ook gelden regels ten aanzien van de technische infrastructuur[26] waarop de politie de gegevens bewaart. De Keuringsdienst controleert, in principe voorafgaand aan een inzet, of een technisch hulpmiddel aan alle eisen voldoet. Indien dat laatste het geval is, wordt een technisch hulpmiddel goedgekeurd. In dat geval mag een technisch hulpmiddel worden gebruikt en hoeft de politie geen uitleg te geven over de werking ervan. De Keuringsdienst kijkt niet naar de technische infrastructuur waarop de gegevens worden opgeslagen.
De eisen uit het Besluit maken dat in Nederland een wettelijk kader bestaat waarin precies geregeld is hoe de kwaliteit van de verzamelde gegevens gewaarborgd dient te worden. De praktijk laat echter zien dat dit in de uitvoeringspraktijk lastig te realiseren is. Hiervoor zijn twee reden. Ten eerste is in de praktijk de ontwikkeling van eigen hulpmiddelen (en ze vooraf goedgekeurd krijgen) nauwelijks haalbaar gebleken in verband met de tijd die het kost om een volledig goedgekeurd middel te ontwikkelen. In de ogen van Digit zijn de regels en eisen die worden gesteld lastig uitvoerbaar, omdat ze niet goed toepasbaar zouden zijn op de technische hulpmiddelen die de politie ontwikkelt. Digit vindt ook niet alle regels noodzakelijk. Als meer geredeneerd zou worden vanuit risicoanalyses en bewijswaardes, zou het niet nodig zijn dat een technisch hulpmiddel aan alle keuringseisen voldoet, zo stelt Digit. Dat is op dit moment wel een wettelijk vereiste. Ten tweede heeft Digit bij het grootste deel van haar inzetten gebruikgemaakt van een commercieel product. Zo'n product schaft de politie aan bij een externe leverancier. Dit product wordt niet onderworpen aan een keuring, omdat de officier van justitie heeft besloten dat de aard van dit middel zich verzet tegen een keuring (een beslissing waarvoor het wettelijk kader ruimte biedt). Op basis van het (huidige) Besluit en de geformuleerde keuringseisen zal dit technisch hulpmiddel ook nooit goedgekeurd kunnen worden. Dit betekent dat ook voor een commercieel product het niet haalbaar is gebleken om een vooraf goedgekeurd technisch hulpmiddel in te zetten. Om de kwaliteit van de gegevens (toch) te kunnen waarborgen zorgt de uitvoeringspraktijk voor aanvullende tactische waarborgen. Deze zijn bedoeld om de gegevens, verkregen met het technisch hulpmiddel, te kunnen verifiëren. In het Besluit wordt er geen rekening mee gehouden dat dat soort maatregelen in de praktijk genomen wordt. Op dit moment is nog niet duidelijk hoe een zittingsrechter de inzetten beoordeelt die met niet gekeurde technische

[25] Besluit onderzoek in een geautomatiseerd werk, 2018.
[26] Een technische infrastructuur is de opslaglocatie voor gegevens die tijdens de uitvoering van een bevel worden vastgelegd (Besluit onderzoek in een geautomatiseerd werk, p. 33).

hulpmiddelen zijn verricht. Voor zover bekend is de inzet van de hackbevoegdheid (tot nu toe) nog géén onderwerp van gesprek geweest tijdens de behandeling van een zaak in de rechtbank. Enkele zaken waarbij een poging is gedaan de hackbevoegdheid in te zetten of de hackbevoegdheid is ingezet zijn wel inmiddels inhoudelijk behandeld in de rechtszaal (zie bijvoorbeeld Berndsen (2022)).[27]

Waarborgen tijdens en na afloop van de inzet

Het Besluit regelt ook een aantal waarborgen tijdens de inzet van de bevoegdheid. De bevoegdheid kan niet door iedereen worden ingezet. Dat geldt bijvoorbeeld voor personen die onderzoekshandelingen met een technisch hulpmiddel mogen verrichten, maar ook voor personen die toegang hebben tot de verzamelde gegevens. Een andere waarborg is logging. Met behulp van logging zou moeten kunnen worden vastgesteld welke handelingen precies zijn uitgevoerd en of zich problemen hebben voorgedaan gedurende de uitvoering van de bevoegdheid. Na afloop van de inzet worden processen-verbaal toegevoegd aan het dossier en dienen personen tegen wie de bevoegdheid is ingezet op de hoogte te worden gesteld. Een persoon hoeft niet apart te worden geïnformeerd indien in zijn of haar dossier via de processen-verbaal terug te lezen is dat de bevoegdheid is ingezet. Tot slot is een laatste waarborg het toezicht door de Inspectie. De Inspectie kijkt naar een groot aantal andere regels in het Besluit en in hoeverre die worden nageleefd. Elke jaar brengt zij hierover een (openbaar) verslag uit. Uit de tot nu toe verschenen Verslagen blijkt dat de politie nog niet aan alle eisen voldoet die op basis van het Besluit aan haar worden gesteld.[28]

[27] Parkins-Ozephius et al. (2022, p. 8-9) merken op dat voor technische hulpmiddelen die vallen onder het 'oude' Besluit Technische Hulpmiddelen Strafvordering al wel verschillende uitspraken zijn. Deze uitspraken wijzen erop dat voor de bewijsvoering het ontbreken van een keuring irrelevant is. De toekomst zal moeten uitwijzen of die beslissingen naar analogie zullen worden toegepast.

[28] In het WODC-rapport (Van Uden & Van den Eeden, 2022) over de Nederlandse uitvoeringspraktijk rondom de hackbevoegdheid wordt ingegaan op de vraag waarom de politie niet altijd aan alle eisen voldoet. Voor dit rapport voert het te ver om hier nader op in te gaan.

3 België[29]

Met speciale dank aan Jan Kerkhofs (Openbaar Ministerie, België) voor het kritische meelezen van dit hoofdstuk op feitelijke onjuistheden.

3.1 Wettelijke regeling

Op 25 december 2016 is in het Belgisch parlement een wet aangenomen die diverse wijzigingen bevat in zowel het Wetboek van Strafvordering als in het Strafwetboek (de zogenoemde 'Cyber-Kerstwet').[30] Deze wet heeft onder meer tot doel de bestaande bijzondere opsporingsbevoegdheden te verbeteren. Twee van die wijzigingen maken het voor de politie mogelijk om te hacken, namelijk de uitbreiding van de inkijkoperatie (een aanpassing van de artikelen 46quinquies Sv en 89ter Sv) en een samenvoeging van de heimelijke zoeking in een 'informaticasysteem'[31] (hierna geautomatiseerd werk) en de onderschepping van telecommunicatie (art. 90ter Sv) (Kerkhofs & Van Linthout, 2019, p. 38-39), hierna data-interceptie.[32] Omdat beide bevoegdheden van een afstand (kunnen) worden uitgeoefend (persoonlijke communicatie, 9 juni 2023; 14 juni 2023), worden ze in dit hoofdstuk uitgebreider besproken. België kent sinds 2019 ook een 'vernieuwd' artikel 88ter Sv. Op basis van dit artikel kan een onderzoeksrechter bevelen een zoeking in een geautomatiseerd werk, begonnen op basis van artikel 39bis Sv, uit te breiden naar een geautomatiseerd werk of naar een deel ervan dat zich op een andere plaats bevindt dan waar de zoeking plaatsvindt. Hiervoor kan de beveiliging van het geautomatiseerd werk worden doorbroken, aangezien artikel 88ter Sv volgens Kerkhofs en Van Linthout (2019, p. 372) samen gelezen dient te worden met paragraaf 5 van artikel 39bis Sv. Aangezien artikel 88ter Sv 'gekaderd dient te worden in de niet-heimelijke internetrecherche' (Kerkhofs & Van Linthout, 2019, p. 394), wordt in dit hoofdstuk dit wetsartikel niet nader besproken.

3.1.1 Inkijkoperatie

Politiediensten mogen, na een machtiging van de onderzoeksrechter, buiten medeweten van de eigenaar of de rechthebbende, of zonder hun toestemming, een private plaats betreden en gesloten voorwerpen die zich op deze plaats bevinden, openen.[33] Een private plaats is een plaats die geen woning is, geen door een woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 Sr en geen lokaal, aangewend voor beroepsdoeleinden, of de woonplaats van een advocaat of een arts als bedoeld in artikel 56bis Sv. Artikel 89ter Sv vormt hierop een aanvulling, zo blijkt uit de eerste paragraaf van dat artikel. Politiediensten mogen een andere private plaats betreden dan die bedoeld in artikel 46quinquies Sv. Ook mag, na een machtiging van de rechter-commissaris, 'buiten medeweten van de eigenaar, de bezitter of de gebruiker of zonder hun toestemming' toegang worden verschaft tot een geauto-

[29] Voor dit hoofdstuk hebben wij dankbaar gebruikgemaakt van Kerkhofs & Van Linthout (2019).
[30] Een deel van deze wet is door het Grondwettelijk Hof vernietigd. Daarom is in mei 2019 reparatiewetgeving aangenomen (Royer & Yperman, 2020, p. 23).
[31] Informaticasystemen zijn, zo volgt uit de voorbereidende werken van de Wet informaticacriminaliteit, 'alle systemen voor de opslag, verwerking of overdracht van data' (Royer & Yperman, 2020, p. 25).
[32] Zie literatuurlijst waarin een verwijzing staat opgenomen naar het Belgisch Wetboek van Strafvordering.
[33] Artikel 46quinquies paragraaf 1 Sv.

matiseerd werk en dat te doorzoeken.[34] In principe kan alleen een onderzoeksrechter een inkijk in het geautomatiseerd werk bevelen. Hierop bestaat één uitzondering. De Procureur des Konings kan een inkijk bevelen in een geautomatiseerd werk, mits dit zich niet bevindt in een woning, of het betreden van de woning daarvoor noodzakelijk is. Bovendien dient het doel van deze inkijk het installeren van een technisch hulpmiddel voor een observatie te zijn, bijvoorbeeld het plaatsen van een keylogger op een computer (persoonlijke communicatie, 24 maart 2023).[35]

Een inkijkoperatie mag alleen plaatsvinden om: (1) 'zich te vergewissen van de eventuele aanwezigheid van zaken die het voorwerp, het middel of het product van het misdrijf of (vervangings-)vermogensvoordelen uit het misdrijf zijn'; (2) 'bewijzen te verzamelen van de aanwezigheid van de bovengenoemde zaken (een gerichte kopie van bepaalde data'); (3) 'een technisch hulpmiddel te plaatsen of weer weg te nemen in het kader van een observatie'; en (4) 'meegenomen voorwerpen terug te plaatsen' (Yperman et al., 2019, p. 397). Voor de inkijkoperatie heeft de wetgever niet vastgelegd op welke wijze kan worden binnengedrongen (bijvoorbeeld door het gebruik van valse sleutels) (Kerkhofs & Van Linthout, 2019, p. 432).

Uit artikel 46quiquies paragraaf 2 sub 1 en 2 Sv blijkt dat de inkijkoperatie mag worden ingezet om zoekend rond te kijken, zowel in de 'reële wereld, als in de virtuele wereld'. Tijdens dit rondkijken is het niet toegestaan om zaken in beslag te nemen (Kerkhofs & Van Linthout, 2019, p. 428). Wel mag worden gekeken of bepaald bewijsmateriaal bestaat en mogen 'enkele stalen' worden genomen. Een gerichte kopie van gegevens zou mogelijk zijn, maar het volledig kopiëren van de harde schrijf niet (Kerkhofs & Van Linthout, 2019, p. 428-429). Vertaald naar de niet digitale wereld betekent het nemen van een staal dat, bijvoorbeeld bij het aantreffen van kilo's cocaïne, een kleine hoeveelheid mag worden meegenomen zodat aangetoond kan worden dat drugs aanwezig is.

3.1.2 Data-interceptie

De tweede bevoegdheid op basis waarvan de politie mag hacken is geregeld in artikel 90ter Sv. De onderzoeksrechter mag 'met een heimelijk oogmerk, niet voor publiek toegankelijke communicatie of gegevens' op een geautomatiseerd werk of een deel ervan met technische hulpmiddelen onderscheppen. Ook mag van deze communicatie of gegevens kennis worden genomen, mogen deze worden doorzocht of mag de zoeking in een geautomatiseerd werk of een deel ervan worden uitgebreid.[36] In het vervolg zal gesproken worden over data-interceptie.

Om data-interceptie mogelijk te maken, zo volgt uit artikel 90ter paragraaf 1 Sv, kan de onderzoeksrechter een bevel afgeven om een woning, private plaats of geautomatiseerd werk binnen te dringen. Vervolgens mag elke beveiliging van het betrokken geautomatiseerd werk tijdelijk worden opgeheven, al dan niet met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden. Tot slot mogen technische hulpmiddelen worden aangebracht in de betrokken systemen om door het systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en

[34] Artikel 89ter Sv.
[35] Dit volgt uit het samenlezen van artikel 89ter, waarin verwezen wordt naar artikel 46quinquies, paragraaf 6 Sv, dat weer verwijst naar artikel 46quinquies, paragraaf 3 Sv (persoonlijke communicatie, 24 maart 2023).
[36] Artikel 90ter paragraaf 1 Sv.

te decoderen. Denk hierbij aan 'het achterlaten van snuffelsoftware of van een remote access tool' (RAT)[37] (Kerkhofs & Van Linthout, 2019, p. 462).

Hoewel beide bevoegdheden (inkijkoperatie en data-interceptie) het voor de politie mogelijk maken om te hacken, vragen Kerkhofs & Van Linthout zich af of de inkijk-operatie (art. 89ter Sv) in praktijk wel gebruikt zal worden. Met een inkijkoperatie zijn veel minder vergaande handelingen mogelijk (zoekend rondkijken en een staal nemen) dan met data-interceptie. Voor beide bevoegdheden geldt echter dat zij op dezelfde (uitgebreide) manier onderbouwd dienen te worden (Kerkhofs & Van Linthout, 2019, p. 431). Bovendien dient voor beide bevoegdheden een volledig gerechtelijk voor-onderzoek te worden gestart (persoonlijke communicatie, 24 maart 2023). Dat roept de vraag op waarom de onderzoeksrechter dan niet direct over zou moeten gaan tot de inzet van data-interceptie (Kerkhofs & Van Linthout, 2019, p. 431).

3.2 Bevoegde autoriteiten

Voor zowel een inkijkoperatie als voor data-interceptie is een machtiging van de onderzoeksrechter vereist die deze 'meedeelt aan de procureur des konings'.[38] In België bestaan, anders dan in Nederland, twee soorten voorbereidend onderzoek: een opsporingsonderzoek en een gerechtelijk vooronderzoek. Het opsporingsonderzoek wordt geleid door een procureur des Konings (PdK). Deze PdK staat aan het hoofd van een arrondissement van het Openbaar Ministerie. Een gerechtelijk vooronderzoek wordt geleid door een onderzoeksrechter (Traest, 2018, p. 25, 29). Een belangrijk verschil tussen beide soorten onderzoek is dat in een opsporingsonderzoek 'behoudens de wettelijke uitzonderingen de opsporingshandelingen in het opsporingsonderzoek geen enkele dwangmaatregel mogen inhouden noch schending van individuele rechten en vrijheden'.[39] Bij een gerechtelijk vooronderzoek kan dat dus wel. In het Belgisch Wetboek van Strafvordering is geen allesomvattende opsomming aanwezig van de bevoegdheden die respectievelijk bij de PdK en bij een onderzoeksrechter zijn ondergebracht. Door het bestaan van de twee soorten vooronderzoek en omdat een aantal onderzoekshandelingen expliciet toegeschreven wordt aan de onderzoeks-rechter, is doorgaans geen onduidelijkheid wie over de inzet van welke bevoegdheid gaat (Traest, 2018, p. 25, 29). De Kamer van inbeschuldigingstelling voert onder andere controle uit over de wijze waarop het gerechtelijk onderzoek verloopt (Ministère Public, z.d.).

Wat betreft de daadwerkelijke uitvoering van de bevoegdheid is op dit moment de inkijkoperatie voorbehouden aan de *National Technical and Support Unit* van de *Dienst Speciale Eenheden* (DSU-NTSU) van de federale politie (Kerkhofs & Van Linthout, 2019, p. 432).

De interceptie van data vindt in principe plaats door gerechtelijke officieren van de politie. Zij kunnen zich laten bijstaan door agenten van de gerechtelijke politie en, onder voorwaarden door de koning bepaald, medewerkers van het administratief en logistiek kader van de geïntegreerde politie.[40] Deze ondersteuning werd nodig geacht,

[37] Een *Remote Access Tool* (RAT) geeft een persoon de mogelijkheid om een computer op afstand binnen te dringen en te beheren.
[38] Artikel 90quater paragraaf 1 Sv; artikel 89ter Sv. Hierop bestaat een uitzondering. De PdK kan zelf een machtiging afgeven voor het inbreken in een geautomatiseerd werk met het oog op het plaatsen (en ook het herstellen en het terugnemen) van een technisch hulpmiddel om een observatie uit te voeren zoals bedoeld in artikel 47sexies paragraaf 1 lid 3 (Kerkhofs, & Van Linthout, 2019, p. 430).
[39] Artikel 28bis paragraaf 3 Sv.
[40] Artikel 90quater paragraaf 3 Sv.

omdat het uitvoeren van de onderzoeksactiviteiten – destijds ging het nog vooral om telefoontaps – te arbeidsintensief was voor alleen de uitvoerende politiediensten (Kerkhofs & Van Linthout, 2019, p. 478). Een deel van de onderzoekswerkzaamheden kan echter niet worden overgelaten aan CaLog-medewerkers.[41] Het gaat daarbij om de analyse van de verzamelde gegevens. Hierop bestaat een uitzondering, namelijk wanneer zij over een bepaalde expertise beschikken. Ook mag deze groep medewerkers niet betrokken worden bij de selectie van de voor het onderzoek van belang geachte delen, zoals bedoeld in artikel 90sexies paragraaf 1 lid 2 Sv.[42] De officieren van de politie moeten namen bijhouden van de personen die hen ondersteunen. Voor elk dossier afzonderlijk wordt een lijst opgesteld volgens nadere regels die de koning bepaalt, na te zijn voorgelegd aan een Commissie die zich bezighoudt met de bescherming van de persoonlijke levenssfeer. Hun namen worden niet opgenomen in het dossier als zij uitvoering geven aan een bevel, zoals bedoeld in artikel 90ter paragraaf 1 Sv.[43] In het Koninklijk Besluit van 17 oktober 2018, gepubliceerd op 19 november 2018, staan voorwaarden genoemd waaraan het CaLog-personeel moet voldoen.[44]

3.3 Tegen wie

Een inkijkoperatie in een geautomatiseerd werk kan alleen plaatsvinden in private omgevingen waarvan op basis van precieze aanwijzingen het vermoeden kan bestaan dat er zaken gevonden kunnen worden zoals bedoeld in artikel 46quinquies paragraaf 2 lid 1 Sv (dat wil zeggen zaken gerelateerd aan een misdrijf). Ook kan een inkijkoperatie plaatsvinden wanneer verwacht wordt dat er bewijzen kunnen worden verzameld of dat de private omgevingen gebruikt worden door verdachten (Kerkhofs & Van Linthout, 2019, p. 431).

Wat betreft data-interceptie moet duidelijk zijn wiens geautomatiseerd werk wordt onderzocht.[45] Dat betekent dat aandacht kan zijn voor de volgende aspecten: de verdachte, de communicatiemiddelen en/of geautomatiseerde werken die de verdachte gebruikt, de plaatsen waar de verdachte zich regelmatig ophoudt en de personen met wie de verdachte in contact staat. Op basis van een uitspraak van het Hof van Cassatie is het voldoende wanneer één van de aspecten vermeld wordt. Dat betekent bijvoorbeeld dat bij een machtiging voor persoon X niet alle telefoons genoemd hoeven worden die persoon X eventueel gebruikt (Kerkhofs & Van Linthout, 2019, p. 452). Dit in tegenstelling tot de Nederlandse situatie (Van Uden & Van den Eeden, 2022, p. 37). Indien gedurende het onderzoek de noodzaak ontstaat om het heimelijk onderzoek op basis van artikel 90ter Sv uit te breiden naar een ander daarmee verbonden geautomatiseerd werk, en dit dient heimelijk plaats te vinden, dan moet er een nieuw bevel

41 Ca-Log is de Franse benaming voor administratief en logistiek kader (Kerkhofs & Van Linthout, 2019, p. 478-479). Ca-Log medewerkers vervullen een burgerfunctie en verrichten administratieve, ondersteunende of technische functies (Jobpol.be, z.d.).

42 Dit betreft: 'de overschrijving of weergave van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicaties of gegevens, en de eventuele vertaling ervan'.

43 Artikel 90quater paragraaf 3 Sv.

44 KB 17 oktober 2018 artikel 1. Twee voorwaarden worden genoemd. Ten eerste moet het personeel zijn aangewezen door de korpschef (bij lokale politie) of door de directeur-generaal gerechtelijke politie of zijn afgevaardigde (bij federale politie). Ten tweede moet er een interne opleiding zijn gevolgd met betrekking tot 'de aanwending van technische hulpmiddelen die worden gebruikt om met een heimelijk oogmerk, niet voor het publiek toegankelijke communicatie of gegevens te onderscheppen, er kennis van te nemen, te doorzoeken en op te nemen of de zoeking in een informaticasysteem (geautomatiseerd werk) of een deel ervan uit te breiden'. Tijdens de opleiding moet aandacht zijn voor 'aspecten inzake gegevensbescherming' (KB 17 oktober 2018, artikel 1).

45 Artikel 90ter paragraaf 1 Sv.

voor data-interceptie komen. Indien het geautomatiseerd werk in een ander land staat, dan dient de procedure in artikel 88ter paragraaf 4 Sv te worden gevolgd (persoonlijke communicatie, 24 maart 2023).

Er bestaat een aparte bepaling hoe met data-interceptie om moet worden gegaan bij geheimhouders.[46] Data-interceptie is bijvoorbeeld alleen toegestaan als de geheimhouder zelf verdacht wordt een strafbaar feit zoals bedoeld in artikel 90ter Sv te hebben gepleegd of verdacht wordt eraan deelgenomen te hebben. Ook kan data-interceptie worden ingezet 'indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd, gebruik maken van diens lokalen, woonplaats, communicatiemiddelen of informaticasystemen'.[47]

3.4 Gevallen

De inkijkoperatie in een geautomatiseerd werk is mogelijk wanneer er ernstige aanwijzingen zijn dat sprake is van een misdrijf zoals bedoeld in artikel 90ter paragrafen 2 t/m 4 Sv. In paragraaf 2 volgt een opsomming van verschillende misdrijven (45 subleden met daarin één of meerdere misdrijven opgenomen). Het gaat bijvoorbeeld om een aanslag op of samenspanning tegen de koning, ernstige schendingen van het humanitair recht, misdaden die door de Grondwet gewaarborgde rechten schenden en bedreiging met een aanslag. Paragraaf 3 betreft een poging tot misdrijven, zoals genoemd in paragraaf 2. Paragraaf 4 is een aanvulling wat betreft 'de vereniging van misdadigers die gevormd is met het doel een aanslag te plegen tegen personen of eigendommen bedoeld in paragraaf 2 of om het in artikel 467 lid 1 bedoelde strafbare feit te begaan'. Het gaat daarbij vooral om diefstallen middels 'braak, inklimming en valse sleutels' (Kerkhofs & Van Linthout, 2019, p. 449). Ook kan de inkijkoperatie worden ingezet wanneer misdrijven gepleegd (zouden) worden in het kader van een criminele organisatie, zoals bedoeld in artikel 324bis van het Strafwetboek (Kerkhofs & Van Linthout, 2019, p. 431).[48] De inzet van deze bevoegdheid is alleen toegestaan 'als overige middelen niet volstaan om de waarheid aan de dag te brengen'.[49]
Data-interceptie op basis van artikel 90ter Sv is mogelijk voor misdrijven die staan opgesomd in paragraaf 2 tot en met 4 van het betreffende artikel (zie hiervoor).

3.5 Termijn

De inkijkoperatie is bedoeld als een eenmalige actie ('one time hit'). Indien het nodig is een geautomatiseerd werk voor een tweede keer binnen te gaan, is een nieuwe machtiging nodig (persoonlijke communicatie, 24 maart 2023). Een machtiging voor data-interceptie wordt afgegeven voor een periode van maximaal één maand. Deze termijn begint op de dag van de machtiging waarbij de inzet van de bevoegdheid wordt bevolen.[50] De startdatum kan met maximaal twee maanden worden opgeschoven tot het moment dat het uitvoeren van de inzet van de bevoegdheid daadwerkelijk begint. Op die manier wordt de tijd die het kost om een geautomatiseerd werk, zoals een telefoon, binnen te komen niet meegerekend voor de periode dat de bevoegdheid mag worden ingezet. Dat kan nodig zijn, omdat het niet

[46] Artikel 90octies.
[47] Artikel 90octies paragraaf 1 Sv.
[48] Artikel 46quinquies paragraaf 1 Sv.
[49] Artikel 46quiquies paragraaf 1 Sv.
[50] Artikel 90quater paragraaf 1 lid 4 Sv.

altijd (technisch) zal lukken om een geautomatiseerd werk binnen te komen (Kerkhofs & Van Linthout, 2019, p. 464). De inzet van de bevoegdheid kan worden verlengd, steeds maximaal met één maand, met een maximale duur van in totaal zes maanden. Deze maximale duur van zes maanden kan met maximaal twee maanden worden verlengd, indien de inzet in verband met technische voorbereidingen later begonnen is.[51]

In de machtiging dienen de 'precieze omstandigheden die de verlenging van de maatregel wettigen' op te worden genomen. Na de periode van zes maanden kan de onderzoeksrechter een nieuwe machtiging afgeven. Dat is mogelijk als zich 'nieuwe en ernstige omstandigheden' voordoen die data-interceptie noodzakelijk maken. In de machtiging dienen de 'precieze nieuwe en ernstige omstandigheden' te worden vermeld die 'een nieuwe maatregel noodzakelijk maken en wettigen'.[52] In de wet is niks geregeld over het maximum aantal verlengingen. Slechts de maximale periode is vastgelegd (Kerkhofs & Van Linthout, 2013, p. 484).

3.6 Formaliteiten

Voor de inkijkoperatie is bepaald dat in spoedeisende situaties de beslissing een private plaats te betreden en gesloten voorwerpen te openen mondeling kan worden medegedeeld. Vervolgens dient de beslissing zo spoedig mogelijk schriftelijk met redenen te worden omkleed en bevestigd te worden.[53]

In de machtiging van de onderzoeksrechter voor de inzet van data-interceptie dient het volgende te worden opgenomen:[54] (1) aanwijzingen en concrete feiten die de maatregel wettigen; (2) redenen waarom de maatregel onontbeerlijk is om de waarheid aan de dag te brengen; (3) de persoon, het communicatiemiddel, het geautomatiseerd werk of de plaats die het voorwerp is van de maatregel; (4) de periode tijdens welke de maatregel kan worden uitgeoefend; en (5) de naam en de hoedanigheid van de officier of officieren van gerechtelijke politie die aangewezen zijn om uitvoering te geven aan de hackbevoegdheid.

De machtiging dient in principe schriftelijk te worden verleend. De onderzoeksrechter kan echter in spoedeisende gevallen de machtiging mondeling verlenen. Binnen 24 uur moet de machtiging schriftelijk worden bevestigd.[55] Ook de PdK kan de data-interceptie mondeling bevelen (als sprake is van een heterdaadsituatie). Wel dient het mondeling bevel zo snel mogelijk op schrift te worden gesteld,[56] in plaats van de maximale 24 uur die voor de onderzoeksrechter geldt.

In artikel 90quater paragraaf 2 en 4 Sv zijn twee medewerkingsplichten opgenomen (Royer & Yperman, 2020, p. 32). Paragraaf 2 regelt dat de onderzoeksrechter de (technische) medewerking kan vorderen van de operator van een elektronisch communicatienetwerk of van aanbieders (op Belgisch grondgebied) van elektronische

[51] Wanneer rekening wordt gehouden met het feit dat de machtiging pas aanvangt als de maatregel daadwerkelijk wordt uitgevoerd, betekent dit dat een verlening maximaal acht maanden kan beslaan. De politie heeft maximaal twee maanden om ervoor te zorgen dat het mogelijk is om een geautomatiseerd werk binnen te komen.
[52] Artikel 90 quinquies Sv.
[53] Artikel 46quiquies paragraaf 1 Sv.
[54] Artikel 90quater paragraaf 1 Sv.
[55] Artikel 90quater paragraaf 1 Sv.
[56] Artikel 90ter paragraaf 5 Sv.

communicatiediensten om de uitvoering van interceptie mogelijk te maken. Boetes kunnen worden opgelegd aan degenen die niet meewerken.

In paragraaf 4 is de tweede medewerkingsplicht opgenomen, namelijk dat de onderzoeksrechter een persoon, van wie vermoed wordt dat deze 'bijzondere kennis' bezit over onder andere het communicatiemiddel, kan vorderen 'inlichtingen te verlenen over de werking' en 'over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud ervan die wordt of is overgebracht'. Ook kan deze persoon gevorderd worden de inhoud toegankelijk te maken. Indien de gevorderde persoon technische medewerking weigert, kan deze gestraft worden met een gevangenisstraf van zes maanden tot één jaar en/of met een geldboete van € 26.000 tot € 20.000. Royer & Yperman (2020, p. 32) concluderen dat de toegevoegde waarde van deze medewerkingsplicht beperkt is, omdat België ook een algemene medewerkingsplicht kent. Deze is geregeld in artikel 88quater Sv.[57]

3.7 Technische hulpmiddelen

In artikel 89ter Sv is niets vastgelegd over de technische hulpmiddelen die gebruikt kunnen worden in het kader van de inkijkoperatie. Bij data-interceptie kunnen technische hulpmiddelen in geautomatiseerde werken worden aangebracht om 'de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen'.[58] Verder is ook voor data-interceptie niets in de wet vastgelegd over de technische hulpmiddelen die mogen worden gebruikt.[59] Informatie hierover is op dit moment ook niet openbaar. Volgens Kerkhofs en Van Linthout (2019, p. 448) biedt de technologie-neutrale formulering 'technisch hulpmiddel' enige armslag aan de politie en het Openbaar Ministerie om creatief te blijven zoeken naar technische tools. Het gaat volgens hen zoals eerder genoemd om het achterlaten van snuffelsoftware of van een remote access tool (RAT) (Kerkhofs & Van Linthout, 2019, p. 462). Uit interviews komt naar voren dat de politie (mogelijk) te gebruiken middelen altijd zelf van tevoren test, onder andere om vast te kunnen stellen of een product doet wat het zou moeten doen. De precieze criteria waarnaar gekeken wordt zijn niet openbaar.

3.8 Waarborgen

3.8.1 Betrouwbaarheid en integriteit van gegevens

'Passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van (…) communicatie of gegevens van een informaticasysteem (geautomatiseerd werk) te waarborgen'.[60] Wat betreft vertrouwelijkheid gaat het volgens Kerkhofs en Van Linthout (2019, p. 491) om de vraag wie welke gegevens mag raadplegen en de wijze waarop met gegevens dient te worden omgegaan (bijvoorbeeld wel of niet verzegeld

[57] Dit artikel kent zowel een informatieplicht als een actieve medewerkingsplicht. De informatieplicht betekent dat er een plicht bestaat 'tot het verstrekken van inlichtingen over de werking van het systeem of de toegang daartoe'. De actieve medewerkingsplicht betekent dat er een plicht bestaat om 'zelf het systeem te bedienen en er bepaalde verrichtingen op uit te voeren' (Conings, 2020, p. 12).

[58] Artikel 90ter paragraaf 1 Sv.

[59] Wel is een definitie opgenomen van een technisch hulpmiddel. Maar, zoals uit de definitie blijkt, gaat die niet op voor de technische hulpmiddelen zoals bedoeld in art. 90ter Sv. 'Een technisch hulpmiddel in de zin van dit wetboek is een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen registreert, met uitzondering van de technische middelen die worden aangewend om een maatregel als bedoeld in artikel 90ter uit te voeren' (Parl. St. Kamer 2015-16, nr. 54 1966/001, 198).

[60] Artikel 90septies paragraaf 1 Sv.

ter beschikking gesteld aan de griffie). Zij geven aan dat dit soort richtlijnen vastgelegd zijn in onder andere artikel 90sexies Sv en artikel 259bis van het Strafwetboek. Daarbij gaat het bijvoorbeeld om de informatie die officieren van de gerechtelijke politie beschikbaar dienen te stellen aan de onderzoekrechter[61] en om straffen die kunnen worden opgelegd wanneer een officier of ambtenaar 'met bedrieglijke opzet (…) gebruik maakt van een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens' afkomstig uit een geautomatiseerd werk.[62]

Wat betreft de integriteit van de gegevens is de Belgische wetgever volgens Kerkhofs & Van Linthout (2019, p. 491) 'zeer op de vlakte gebleven'. De wetgever spreekt alleen over 'passende middelen',[63] maar er wordt verder niet uitgelegd wat daaronder precies verstaan wordt. Het is vervolgens aan de verdediging om (tijdens de behandeling van de rechtszaak) de middelen die zijn ingezet (beschreven in het dossier, zie later) ter discussie te stellen, inclusief de vraag of het bewijs dat gepresenteerd wordt betrouwbaar en integer is. Het is uiteindelijk de zittingsrechter die hierover een besluit neemt. Verder dient de politie een zo goed mogelijke uitleg te geven, zonder daarbij opsporingstactieken prijs te geven, hoe zij aan bepaalde gegevens is gekomen en dat er geen wijzigingen hebben plaatsgevonden of hebben kunnen plaatsvinden van de verzamelde gegevens. Dat zou kunnen gebeuren met het berekenen van hashwaardes[64] wanneer het gaat om gegevens die inbeslaggenomen zijn (Kerkhofs & Van Linthout, 2019, p. 491-492). In één van de interviews komt naar voren dat het gebruik van hashes geen standaardpraktijk is. Wel worden Etsi-normen gehanteerd. Etsi speelt een belangrijke rol bij het ondersteunen van wetgeving en andere regelgeving met betrekking tot technische (ICT-)standaarden en specificaties (Etsi, z.d.; Etsi, 2020). Er zijn bijvoorbeeld standaarden geformuleerd voor wettelijke interceptie ('*lawful interception*') (Etsi, z.d.b). Op welke wijze deze normen concreet vorm krijgen met betrekking tot de technische hulpmiddelen die gebruikt worden voor het uitvoeren van data-interceptie, is gedurende dit onderzoek niet precies duidelijk geworden. Verder, zo komt tijdens datzelfde interview naar voren, zet de politie doorgaans meerdere opsporingsbevoegdheden in waardoor de met behulp van de hackbevoegdheid verzamelde gegevens niet het enige bewijs zijn.

3.8.2 Verslaglegging

Om de kwaliteit van de verzamelde gegevens te controleren is nog een aantal andere maatregelen relevant, namelijk de wijze waarop verslaglegging plaatsvindt en de dossiervorming.
Wat betreft de inkijkoperatie dient de officier van de gerechtelijke politie, die de uitvoering van de bevoegdheid leidt, een proces-verbaal op te stellen. Dit proces-verbaal wordt aan het strafdossier toegevoegd, uiteindelijk nadat de inzet van de bevoegdheid is beëindigd. Als bij het uitvoeren van de bevoegdheid een voorwerp meegenomen moet worden,[65] dan dient dat vermeld te worden in het proces-verbaal.[66]
Wat betreft data-interceptie regelt artikel 90quater paragraaf 3 Sv dat de officieren van de gerechtelijke politie tenminste om de vijf dagen schriftelijk verslag uitbrengen

[61] Artikel 90sexies Sv paragraaf 1 lid 1 Sv.
[62] Artikel 259bis paragraaf 2 Sr.
[63] Artikel 90septies paragraaf 1 Sv.
[64] Met een hash wordt een unieke code berekend op basis van de (set van) data. Als op een later moment (op het moment dat de data ergens anders staan) de hash opnieuw wordt berekend en deze hetzelfde is als de eerder berekende hashwaarde, dan is dat een aanwijzing dat aan de data niets veranderd is. Een hash zorgt ervoor dat de integriteit van de gegevens is gewaarborgd (Van Uden & Van den Eeden, 2022, p. 114).
[65] Artikel 46 quinquies paragraaf 5 Sv.
[66] Artikel 46 quinquies paragraaf 7 Sv.

aan de onderzoeksrechter over de uit te voeren machtiging. In artikel 90sexies paragraaf 1 Sv is verder vastgelegd wat de politie aan de onderzoeksrechter dient te overhandigen. Het gaat daarbij ten eerste om een bestand met daarin de opgenomen communicatie of gegevens.[67] Ten tweede 'de overschrijving of weergave van de door de aangewezen officieren van gerechtelijke politie voor het onderzoek van belang geachte gedeelten van de opgenomen communicatie of gegevens', en een eventuele vertaling. Ten derde indien relevant 'de plaats van de gegevens bedoeld in de bepaling onder lid 2 in het informaticasysteem' (geautomatiseerd werk) en ten vierde 'een algemene beschrijving van de inhoud en van de identificatiegegevens van de gebruikte communicatiemiddelen of informaticasystemen wat betreft de niet van belang geachte communicatie of gegevens'.

Kerkhofs & Van Linthout (2019, p. 482) merken op dat het bij het onderscheppen van digitale informatie niet mogelijk zal zijn om een onderzoeksrechter elke vijf dagen inhoudelijk op de hoogte te brengen. Er zal doorgaans een grote hoeveelheid informatie worden verzameld die eerst nog moet worden geïnterpreteerd. Dat betekent dat het toezicht door de onderzoeksrechter enigszins vertraging zal oplopen. Wel moet de onderzoeksrechter op basis van de vijfdaagse verslagen in staat worden gesteld om te beoordelen of de inzet van de bevoegdheid nog doorgang kan vinden of dat deze (vroegtijdig) dient te worden beëindigd. De onderzoeksrechter bepaalt uiteindelijk ook welke selectie van gegevens van belang is voor het onderzoek.[68]

3.8.3 Samenstelling dossier en inzage

Het strafdossier van een zaak waarin de bevoegdheid tot data-interceptie is ingezet bevat drie soorten stukken: (1) de machtigingen door de onderzoeksrechter en eventuele verlengingen; (2) de vijfdaagse verslagen; en (3) processen-verbaal die gaan over de daadwerkelijke uitvoering van de bevoegdheid. Deze stukken worden uiterlijk na het beëindigen van de inzet van de bevoegdheid aan het dossier toegevoegd.[69] De onderzoeksrechter bepaalt welke selectie van gegevens van belang is voor het onderzoek.[70] Er zijn geen vormvoorschriften verbonden aan de manier waarop gegevens geselecteerd dienen te worden (Kerkhofs & Van Linthout, 2019, p. 483). Wat betreft het noemen van namen van personen die op de een of andere manier betrokken zijn bij de interceptie merken Kerkhofs & Van Linthout (2019, p. 480) op dat de wetgever niet duidelijk is welke namen wel en welke namen niet genoemd dienen te worden. In de memorie van toelichting wordt aangegeven dat namen van ondersteunende medewerkers, zoals CaLog-medewerkers (zie paragraaf bevoegde autoriteiten) niet vermeld hoeven te worden. De wet stelt echter[71] dat alleen de namen van de personen die zich bezighouden met het daadwerkelijk hacken niet hoeven te worden vermeld in het gerechtelijk dossier. Volgens Kerkhofs & Van Linthout (2019, p. 480) dienen om die reden wel de namen van andere personen dan

---

67 In de praktijk gaat het hier om een dvd die door de politie (NTSU-CTIF) wordt gebrand. In de wet is voorzien dat de Koning een dienst kan aanwijzen waarbij de gegevens ook bewaard worden (naast bij de griffie). Daarbij gaat het om een aanvullende kopie, zodat de kans verkleind wordt dat gegevens verloren gaan. Deze dienst zou voldoende waarborgen moeten kunnen bieden dat opnames op zo'n manier worden bewaard dat ze voor een langere periode 'intact' blijven en dat onbevoegde personen er geen toegang toe krijgen (Kerkhofs & Van Linthout, 2019, p. 489). De noodzakelijke waarborgen dienen vastgesteld te worden door de Koning (Parl. St. Kamer 2015-16, nr. 54 1966/001, 71).

68 Artikel 90sexies paragraaf 2 Sv.

69 Artikel 90sexies paragraaf 4 Sv. Voor artikel 89ter Sv is dit niet op deze manier geregeld. In dat geval is er alleen de machtiging en het proces-verbaal van de uitvoering en eventueel verdere processen-verbaal met betrekking tot hetgeen al dan niet is aangetroffen en/of geanalyseerd is (persoonlijke communicatie, 24 maart 2023).

70 Artikel 90sexies paragraaf 2 Sv.

71 Artikel 90quater paragraaf 3 Sv.

de hackers vermeld te worden. Alleen op die manier kan de onderzoeksrechter in de gaten houden of een 'privacy zeer invasieve maatregel' als data-interceptie[72] 'onder controle blijft en niet zomaar iedereen kennis kan nemen' van de gegevens die met behulp van die bevoegdheid verzameld worden. Een beperkt aantal betrokkenen bij de uitvoering is een 'bijkomende waarborg voor confidentialiteit', zo blijkt volgens Kerkhofs & Van Linthout (2019, p. 480) uit de memorie van toelichting op het 'Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privécommunicatie en telecommunicatie (*Parl. St.* Senaat 1992-93, 843-1, 16). In het Koninklijk Besluit van 17 oktober 2018, artikel 3, is dat echter niet op die manier geregeld volgens Kerkhofs & Van Linthout (2019, p. 480). Uit dat artikel blijkt volgens hen dat er geen rechtstreekse controle meer is door de onderzoeksrechter, maar alleen door de politie zelf.

Alle gebruikte stukken die niet aan het dossier worden toegevoegd, worden óf vernietigd óf naar de griffie gestuurd. Kerkhofs & Van Linthout (2019, p. 488) vragen zich af of op die manier voldoende controle kan plaatsvinden. Het is immers uiteindelijk maar een kleine selectie van stukken die in het dossier belandt. De volgende stukken worden vernietigd: 'Iedere aantekening [die] in het kader van de tenuitvoerlegging van de maatregelen bedoeld in de artikelen 90ter, 90quater en 90quinquies door de daartoe aangewezen personen [wordt gemaakt] (…)'.[73] In artikel 90septies paragraaf 4 Sv is vastgelegd welke stukken (aan het begin van deze paragraaf reeds opgesomd) onder verzegelde omslag bij de griffie worden bewaard.

Gegevens die geïntercepteerd worden op basis van artikel 90ter Sv hoeven niet meer volledig uitgewerkt te worden. Een selectie ervan in het dossier volstaat. Wel zijn de mogelijkheden vergroot om het toezicht op die selectie uit te kunnen voeren. In artikel 90septies paragraaf 6 lid 1 Sv wordt bepaald dat 'de inverdenkinggestelde, de burgerlijke partij of hun raadslieden' op verzoek een kopie ontvangen van de opgenomen gegevens waarvan een gedeelte ervan zich bevindt in het proces-verbaal. Het kan voorkomen dat de verzoekende partij, bijvoorbeeld een raadsman/-vrouw, wil dat een deel van de door hem of haar opgevraagde gegevens aan het dossier worden toegevoegd. In dat geval dient een verzoek te worden gedaan aan de (onderzoeks-) rechter. Als een raadsman-/vrouw het verzoek doet aan de onderzoekrechter, dan zal deze het verzoek behandelen overeenkomstig artikel 61quinquies Sv, zo blijkt uit artikel 90septies paragraaf 6 Sv. In dat laatste artikel zijn ook drie redenen genoemd waarom een rechter het verzoek kan afwijzen: (1) indien hij/zij de toevoegingen niet noodzakelijk acht om de waarheid aan de dag te brengen; (2) indien de toevoeging op dat moment nadelig wordt acht voor het onderzoek; en (3) vanwege de bescherming van andere rechten of belangen van personen.

In het kader van de wetgeving voorlopige hechtenis krijgen verdachten, zodra zij worden aangehouden, inzage in het gerechtelijk vooronderzoek. Dat kan betekenen dat een verdachte ook al inzicht zou kunnen krijgen in lopende inzetten van opsporingsbevoegdheden zoals data-interceptie, bijvoorbeeld bij andere verdachten. Om dat te voorkomen is het eerdergenoemde artikel 90sexies paragraaf 4 Sv in het leven geroepen. Daarin wordt geregeld dat machtigingen van de onderzoeksrechter, verslagen van officieren van gerechtelijke politie en processen-verbaal die betrekking hebben op de inzet van de bevoegdheid, uiterlijk na het beëindigen van de inzet aan het dossier worden toegevoegd (Kerkhofs & Van Linthout, 2019, p. 490).

[72] Artikel 90ter Sv.
[73] Artikel 90septies paragraaf 3 Sv.

3.8.4 Notificatieplicht

Iedere persoon ten aanzien van wie de bevoegdheid tot data-interceptie (art. 90ter Sv) is ingezet, dient schriftelijk in kennis te worden gesteld van de aard van de inzet van de bevoegdheid en de dagen waarop de bevoegdheid is ingezet.[74] Uiterlijk vijftien dagen nadat de beslissing over de regeling van rechtspleging definitief is geworden en nadat de dagvaarding ter griffie van de rechtbank of het Hof werd neergelegd, brengt de griffier de persoon ten aanzien van wie de bevoegdheid is ingezet op de hoogte. Dat doet de griffier op vordering van de PdK of in voorkomend geval op vordering van de procureur-generaal. Er geldt een uitzondering op de plicht tot notificatie, namelijk wanneer de identiteit of woonplaats redelijkerwijs niet achterhaald kan worden.

3.8.5 Extern toezicht

Naast de controle die plaatsvindt door de magistratelijke autoriteiten, kent België een comité P (Vast Comité van Toezicht op de politiediensten). Dit comité is geïntroduceerd in de 'Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse' van 18 juli 1991, hierna Wet toezicht op politie. Comité P is een 'externe instelling die onder de begeleiding van het federaal parlement belast is met het toezicht op de globale werking van de politie-, inspectie- of handhavingsdiensten' (Comité P, z.d.). Comité P houdt geen toezicht op gerechtelijke overheden, handelingen die zij bij de uitvoering van strafvordering stellen en op overheden van bestuurlijke politie.[75] Comité P kijkt wel naar 'de uitoefening van de politiefunctie door alle bevoegde ambtenaren'. Zij richt zich verder onder andere op de manier waarop 'fundamentele rechten en vrijheden worden nageleefd en actief worden gestimuleerd' (Comité P, z.d.). Comité P schrijft onder andere jaarverslagen en cahiers. In de jaarverslagen en cahiers gepubliceerd door comité P is voor zover bekend geen informatie te vinden over het gebruik van data-interceptie en de inkijkoperatie. Verder zijn er geen aanwijzingen dat het comité zich daar binnenkort op zal richten.

3.9 Jurisprudentie

De Minister van Justitie brengt elk jaar een jaarverslag uit over de artikelen 90ter tot en met 90novies Sv.[76] Het parlement dient op de hoogte te worden gebracht van het aantal onderzoeken die in het kader van deze artikelen zijn ingezet, de duur van de betreffende maatregelen, het aantal betrokken personen en de behaalde resultaten. Dit verslag is niet openbaar. Bovendien is het op basis van dit verslag niet goed mogelijk om te achterhalen hoe vaak artikel 90ter is ingezet. Binnen artikel 90ter Sv valt immers ook de 'gewone' telefoontap.

Wat betreft de beschikbare jurisprudentie wordt het hacken zelf zelden ter discussie gesteld in de rechtszaal (persoonlijke communicatie, 24 maart 2023). Eén van de geïnterviewden geeft aan dat het hierbij gaat om de wijze waarop de hack heeft plaatsgevonden.

[74] Artikel 90novies Sv. Deze voorwaarde is niet voorgeschreven op straffe van nietigheid en wordt niet altijd even stipt toegepast (persoonlijke communicatie 24 maart 2023).
[75] Artikel 2 Wet toezicht op politie.
[76] Artikel 90decies Sv.

3.10 Tot slot

België kent twee wetsartikelen die het de politie toestaat om een geautomatiseerd werk binnen te dringen: artikel 89ter Sv en artikel 90ter Sv. Op basis van artikel 89ter Sv mag een speciaal team van de Belgische politie een geautomatiseerd werk doorzoeken en een 'staal' van gegevens nemen (de 'inkijkoperatie'). Artikel 90ter Sv maakt het voor de politie mogelijk een geautomatiseerd werk binnen te gaan en daaruit gegevens op te halen (data-interceptie). Met de tweede bevoegdheid mag de politie (veel) meer informatie binnen halen dan met een inkijkoperatie.

In de wet is weinig vastgelegd over technische hulpmiddelen en eventuele eisen die daaraan gesteld worden, bijvoorbeeld met betrekking tot de kwaliteit van de gegevens. Eén van de weinige dingen die genoemd wordt is dat een technisch hulpmiddel mag worden gebruikt. Wat betreft de criteria waaraan zo'n technisch hulpmiddel moet voldoen is alleen vastgelegd dat passende middelen aangewend moeten worden om de integriteit en de vertrouwelijkheid van de verzamelde gegevens te waarborgen. Wat precies onder 'passend' moet worden verstaan, is verder niet duidelijk. Hetzelfde geldt voor de vraag wie deze passendheid zou moeten controleren. In de praktijk test de politie zelf de technische hulpmiddelen. Daarnaast worden meerdere bevoegdheden tegelijkertijd gebruikt waardoor in het dossier niet alleen geleund hoeft te worden op gegevens die zijn verzameld middels data-interceptie.

In België is iets meer geregeld gedurende de inzet van de bevoegdheid, maar vooral na afloop van de inzet. Voor de vertrouwelijkheid van gegevens geldt een aantal voorwaarden, bijvoorbeeld ten aanzien van wie gegevens mag raadplegen, waar deze worden opgeslagen (bij een griffie) en voor wie die gegevens vervolgens toegankelijk zijn. Dat betekent dat in theorie niet zomaar iedereen bij de verzamelde gegevens kan. Wetgeving hieromtrent zou echter niet eenduidig zijn waardoor er maar beperkte controle is wie allemaal toegang heeft gehad tot de gegevens. Die controle ligt niet bij een onderzoeksrechter, maar bij de politie zelf. Een andere vorm van controle zijn de vijfdaagse verslagen die aan de onderzoeksrechter overhandigd dienen te worden. Dat betekent dat een onafhankelijke partij controle houdt op de uitvoering. Die controle zal overigens altijd wat achterlopen op de voortgang van het daadwerkelijke onderzoek, omdat het verwerken van de verzamelde gegevens veel tijd kost in verband met de grote hoeveelheid data die binnenkomt. Tot slot is vooral een controlemogelijkheid ingebouwd nadat de gegevens zijn verzameld en een verdachte en de verdediging toegang krijgen tot het dossier en de zaak door een rechter wordt behandeld. Aan de hand van het dossier zou de verdediging de gebruikte middelen ter discussie kunnen stellen door hierover vragen te stellen. Daarbij is het wel de vraag hoeveel informatie zal worden prijsgegeven, omdat doorgaans geen mededelingen worden gedaan over de exacte werking van een technisch hulpmiddel. Daarbij komt dat niet alle gegevens automatisch worden toegevoegd aan het dossier. Wel kan de verdediging, onder voorwaarden, zicht krijgen op de (volledigheid van de) verzamelde gegevens en een verzoek doen om gegevens toe te voegen aan het dossier.

4 Duitsland

Met speciale dank aan Rainer Franosch (ministerie van Justitie, Duitsland) voor het kritische meelezen van dit hoofdstuk op feitelijke onjuistheden.

4.1 Wettelijke regeling

Op 24 augustus 2017 is in Duitsland een wet in werking getreden om de strafrechtelijke rechtshandhaving effectiever en in de praktijk bruikbaar te maken (‘*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*‘) (Bundesministerium der Justiz, z.d.). Deze wet wijzigde onder meer het Duitse Wetboek van Strafvordering (Sv), de ‘*Strafprozeßordnung’*. Er werden twee mogelijkheden gecreëerd voor opsporingsinstanties om te hacken met het doel de opsporing en vervolging van strafbare feiten (Škorvánek, Koops, Newell, & Roberts, 2020, p. 1012-1013).[77] Op basis van de wijzigingen mag de politie telecommunicatie bij de bron onderscheppen (hierna broninterceptie)[78] en een online doorzoeking in een informatietechnologiesysteem (hierna geautomatiseerd werk) uitvoeren)[79] ‘*Online-Durchsuchung’*).[80]

De splitsing van broninterceptie en de online doorzoeking komt voort uit de beslissing van het Grondwettelijk Hof, het ‘*Bundesverfassungsgericht’* (hierna BVerfG),[81] uit 2008 (Bundesverfassungsgericht, z.d.) (Škorvánek et al., 2020, p. 1013). De BVerfG velde een oordeel over een wet uit Noordrijn-Westfalen op basis waarvan opsporingsautoriteiten in deze deelstaat heimelijk op afstand computers van verdachten konden doorzoeken (Groothuis, 2008, p. 990). De BVerfG verklaarde de online doorzoeking nietig, en oordeelde dat de inzet van de bevoegdheid onverenigbaar was met het persoonlijkheidsrecht, in samenhang met het grondrecht op de menselijke waardigheid (art. 2 (1) Gw juncto artikel 1 (1) Gw), met het telecommunicatiegeheim (art. 10 (1) Gw) en met de inperking van grondrechten (art. 19 (1) Gw) (zie ook Groothuis, 2008, p. 990-991). Deze beslissing heeft er onder meer voor gezorgd dat het persoonlijkheidsrecht (‘*allgemeine Persönlichkeitsrecht’*)[82] werd uitgebreid met het recht op de bescherming van de vertrouwelijkheid en integriteit van informatietechnologiesystemen (Groothuis, 2008, p. 990). Hoe uitgebreider een bevoegdheid inbreuk maakt op het privéleven van een individu, hoe zwaarder de voorwaarden moeten zijn voor de

[77] Naast het Wetboek van Strafvordering, zijn er nog drie andere wettelijke grondslagen op basis waarvan kan worden gehackt. Ten eerste kan de Duitse federale politie preventief hacken op basis van de ‘*Bundeskriminalamtgesetz’* (BKAG). Zie voor de broninterceptie artikel 51 lid 2 BKAG en voor de online doorzoeking artikel 49 BKAG. De BKAG regelt de taken en bevoegdheden van de federale politie, die zich met name bezighoudt met criminaliteit als terrorisme en mensenhandel (Fedorova, Te Molder, Dubelaar, Lestrade, & Walree, 2022, p. 128). Ten tweede, in de politiewet van enkele deelstaten (‘*Bundesländer’*) is een preventieve hackbevoegdheid neergelegd (Škorvánek et al., 2020, p. 1012). Ten derde is er voor de opsporingsdienst van de douane, de ‘*Zollkriminalamt’* een hackbevoegdheid neergelegd in artikel 72 lid 3 van de ‘*Zollfahndungsdienstgesetz’*. In dit rapport beperken wij ons tot de bespreking van de twee mogelijkheden die in het Wetboek van Strafvordering staan opgenomen.

[78] § 100a (1) tweede en derde zin Sv.

[79] § 100b (1) Sv.

[80] Broninterceptie richt zich op communicatie en de online doorzoeking op gegevens. Zie voor een uitgebreidere uitleg, paragrafen 4.1.1 en 4.2.2.

[81] De BverfG is de hoogste rechterlijke instantie in Duitsland die wetgeving toetst aan de Grondwet. De BverfG kan ook uitspraak doen in strafzaken in het geval van een (mogelijke) schending van de Grondwet (Klip, Peristeridou, & De Vocht, 2019, p. 35).

[82] Het persoonlijkheidsrecht houdt in dat ieder individu zijn of haar persoonlijkheid kan ontwikkelen (artikel 2 lid 1 Gw juncto artikel 1 lid 1 Gw).

inzet daarvan (Deutscher Bundestags, 2017, p. 47).[83] Met behulp van online doorzoekingen kunnen opsporingsinstanties een uitgebreid persoonlijkheidsprofiel van burgers maken (Groothuis, 2008, p. 1001). Uitgebreider dan dat het geval is bij het onderscheppen van telecommunicatie. Bij dat laatste wordt enkel inbreuk gemaakt op het telecommunicatiegeheim uit artikel 10 Gw, waaraan minder zwaarwegende waarborgen zijn verbonden. Omdat de mate waarin de bevoegdheden een inbreuk maken op de persoonlijke levenssfeer verschilt, zijn de bevoegdheden in twee aparte wettelijke bepalingen neergelegd (Škorvánek et al., 2020, p. 1013).

4.1.1 Bronintercepție van telecommunicatie

In 2017 is de bestaande interceptiebevoegdheid van § 100a Sv uitgebreid met een extra bepaling die bronintercepție mogelijk maakt (in de tweede en derde zin van lid 1). Vóór 2017 konden opsporingsinstanties op basis van het oude § 100a Sv al communicatie, zoals telefoongesprekken, faxen en e-mails, onderscheppen en opnemen buiten medeweten van de verdachte (‘*Telekommunikationsüberwachung*’). Voor de uitvoering hiervan werd de hulp ingeschakeld van telecommunicatiebedrijven en internetproviders (Niedernhuber, 2018, p. 170). Met behulp van deze traditionele bevoegdheid kan echter niet de inhoud van versleutelde communicatie worden achterhaald. Dat is met de nieuwe bepaling wel mogelijk (Deutscher Bundestags, 2017, p. 49). Op basis van het nieuwe § 100a Sv mogen opsporingsinstanties met behulp van een technisch hulpmiddel het geautomatiseerd werk van de verdachte, zoals een laptop, een tablet of een mobiele telefoon (Niedernhuber, 2018, p. 170) binnendringen. Het binnendringen op een geautomatiseerd werk zorgt ervoor dat de politie, voordat communicatie wordt versleuteld of nadat communicatie is ontsleuteld, deze communicatie ‘op de bron’ mee kan lezen en kan opnemen.[84] Bij telecommunicatie gaat het onder andere om gesprekken via Skype en berichten verstuurd via berichtendiensten zoals WhatsApp en Telegram (Niedernhuber, 2018, p. 170; Singelnstein & Derin, 2017, p. 2647).[85] Opsporingsinstanties mogen geen camera of microfoon aanzetten, of gegevens wijzigen (Niedernhuber, 2018, p. 172). Wel mogen opsporingsinstanties de inhoud en de omstandigheden van de communicatie, opgeslagen in het geautomatiseerd werk van de verdachte, onderscheppen en opnemen. Dit zijn opgeslagen gegevens gerelateerd aan telecommunicatie uit het verleden (Škorvánek et al., 2020, p. 1014), waaronder ook metadata. Een voorwaarde hierbij is dat opsporingsinstanties deze gegevens ook tijdens het transmissieproces in het openbare telecommunicatienetwerk op een versleutelde manier hadden moeten kunnen onderscheppen en opnemen.[86] Dit is een belangrijk verschil met de online doorzoeking (zie volgende paragraaf). Met bronintercepție mag alleen communicatie worden binnengehaald die er was op het moment dat een bevel werd afgegeven (Deutscher Bundestags, 2017, p. 50).

4.1.2 Online doorzoeking

De tweede bevoegdheid die het voor opsporingsinstanties mogelijk maakt om te hacken is de online doorzoeking. Op basis van § 100b (1) Sv kunnen opsporingsinstanties, met gebruik van technische hulpmiddelen, heimelijk toegang krijgen tot het geautomatiseerd werk van de verdachte en hier gegevens uithalen. In principe krijgen

[83] Dit staat ook wel bekend als het ‘Kernbereich privater Lebensgestaltung’-concept (Lindemann & Van Toor, 2018).
[84] § 100a (1) tweede zin Sv.
[85] In de wetenschappelijke literatuur wordt gediscussieerd over wat verder onder telecommunicatie wordt verstaan. Zie bijvoorbeeld Niedernhuber (2018) en Singelnstein & Derin (2017).
[86] § 100a (1) derde zin Sv.

opsporingsinstanties toegang tot alle gegevens die zijn opgeslagen op het geautomatiseerd werk van de verdachte. Zij kunnen ook berichten lezen die zijn verstuurd voordat toestemming gegeven was voor de online doorzoeking (Deutscher Bundestags, 2017, p. 50; Niedernhuber, 2018, p. 171). Vanwege de terminologie die in de wettekst wordt gebruikt, die refereert aan het halen van opgeslagen gegevens uit een geautomatiseerd werk, concluderen diverse auteurs dat opsporingsinstanties niet de camera of microfoon van het geautomatiseerd werk van de verdachte mogen activeren om video- of geluidopnames te maken (Lindemann & Van Toor, 2018, p. 381; Niedernhuber, 2018, p. 172; Singelnstein & Derin, 2017, p. 2647). Ook mogen zij geen opgeslagen gegevens wijzigen (Niedernhuber, 2018, p. 172; Singelnstein & Derin, 2017, p. 2647). Bovendien moet de inzet van de bevoegdheid beperkt blijven tot de gegevens die relevant zijn voor de strafzaak in kwestie. Een uitgebreid onderzoek van het gehele geautomatiseerd werk is ontoelaatbaar (Singelnstein en Derin, 2017, p. 2647).

In de wet is de exacte wijze waarop opsporingsinstanties een geautomatiseerd werk kunnen binnendringen niet vastgelegd. Dat moeten zij doen met behulp van technische hulpmiddelen of middels een '*kriminalistischer List'* (bijvoorbeeld *social engineering*). Verder is er geen wettelijke grondslag voor opsporingsinstanties om heimelijk een fysieke plaats, zoals de woning van een verdachte, te betreden om vervolgens diens geautomatiseerd werk binnen te dringen (Deutscher Bundestags, 2017, p. 52).

4.2 Bevoegde autoriteiten

De uitvoering van broninterceptie en de online doorzoeking vindt plaats bij de '*Bundeskriminalamt'*, de Duitse federale recherchedienst (hierna BKA) (Deutscher Bundestags, 2017, p. 52). In principe mag elke competente politieautoriteit deze bevoegdheden uitvoeren. In de praktijk beschikken niet alle politieonderdelen over de juiste middelen. De officier van justitie beslist welk politieonderdeel de bevoegdheid uitvoert (persoonlijke communicatie, 23 mei 2023). Uit één van de interviews blijkt dat in de praktijk het forensisch team van de politie de broninterceptie en de online doorzoeking uitvoert. Overige opsporingsteams kunnen bij dit team aankloppen voor de inzet van beide bevoegdheden.

Voor beide bevoegdheden is een vorm van magistratelijke toetsing vereist, zoals beschreven in § 100e Sv. In het geval van de broninterceptie moet een onderzoeksrechter toestemming geven voor de inzet van de bevoegdheid (een gerechtelijk bevel), na een verzoek van het Openbaar Ministerie. Wanneer er dringende omstandigheden zijn, kan het Openbaar Ministerie direct een bevel afgeven (zonder voorafgaande toestemming van een rechter). Wel moet de inzet van de bevoegdheid binnen drie werkdagen door een rechter worden goedgekeurd.[87] In het geval van de online doorzoeking dient het Openbaar Ministerie een verzoek in bij de *'Kammer des Landgerichts'*[88] die een eventuele inzet moet goedkeuren.[89] Het betreft een '*Staatsschutz'* kamer van een regionale rechtbank, bestaande uit drie rechters (Soiné, 2018,

[87] § 100e (1) Sv.
[88] Het Landgericht in het arrondissement waar het Openbaar Ministerie is gevestigd, is bevoegd om autorisatie te verlenen voor de inzet van de bevoegdheid zoals gespecificeerd in artikel 74a lid 4 van de '*Gerichtsverfassungsgesetzes'* (§ 100e lid 2 Sv).
[89] § 100e (2) Sv.

p. 496).[90] Dat een rechtbank beslist over de inzet betekent dat, in tegenstelling tot bronintercepte, meerdere rechters betrokken zijn bij de autorisatie van de online doorzoeking, zo blijkt uit enkele interviews. Wanneer er dringende omstandigheden zijn, kan de voorzitter van de Kammer (‘*Vorsitzenden*’) een bevel uitgeven. De regionale rechtbank moet de bevoegdheid dan nog binnen drie werkdagen goedkeuren.

4.3 Tegen wie

Beide bevoegdheden (bronintercepte en de online doorzoeking) dienen in beginsel gericht te worden ingezet. Bronintercepte moet betrekking hebben op de communicatie van een verdachte. Ook mag de politie personen aftappen van wie op grond van bepaalde feiten kan worden aangenomen dat zij berichten ontvangen of versturen die bestemd zijn voor of afkomstig zijn van de verdachte. Verder mag deze bevoegdheid worden ingezet ten aanzien van andermans telefoonaansluiting of geautomatiseerd werk dat de verdachte gebruikt.[91] Ook de online doorzoeking is in principe op de verdachte gericht. Opsporingsinstanties mogen daarnaast systemen van andere personen binnendringen, mits op grond van bepaalde feiten kan worden aangenomen dat de verdachte het geautomatiseerd werk van die ander(-en) gebruikt èn als het binnendringen in het geautomatiseerd werk van de verdachte niet leidt tot het vaststellen van de feiten of tot het bepalen van de verblijfplaats van een medeverdachte.[92]

4.4 Gevallen

Bronintercepte is mogelijk wanneer het vermoeden bestaat dat de verdachte, als dader of als medeplichtige, een ernstige vorm van criminaliteit (‘*schwere Straftat*’) heeft gepleegd. Deze ernstige vormen van criminaliteit staan limitatief opgesomd in § 100a (2) Sv. Het gaat bijvoorbeeld om afpersing, drugsgerelateerde misdrijven en witwassen. Ook kunnen opsporingsinstanties telecommunicatie onderscheppen indien sprake is van een verdenking van een poging tot of van de voorbereiding van een ernstige vorm van criminaliteit.[93] Om een online doorzoeking te mogen doen, moet een verdenking bestaan van een zeer ernstige vorm van criminaliteit (‘*besonders schwere Straftat*’). In § 100b (2) Sv volgt een limitatieve opsomming van deze vormen van criminaliteit, waaronder georganiseerde criminaliteit, moord met verzwaarde omstandigheden en mensenhandel. De online doorzoeking is ook toegestaan indien sprake is van een poging tot of van voorbereidingshandelingen van een zeer ernstige vorm van criminaliteit.[94]

4.5 Termijn

De bronintercepte kan voor maximaal drie maanden worden gemachtigd. De inzet van de bevoegdheid mag steeds met drie maanden worden verlengd. Dat mag enkel als, rekening houdend met de informatie die in de loop van het onderzoek is verzameld, de

[90] De rechterlijke macht in Duitsland kent de volgende indeling: lokale rechtelijke instantie (‘*Amtsgerichte*’), regionale gerechtelijke instantie (‘*Landgerichte*’), hogere regionale gerechtelijke instantie (‘*Oberlandesgerichte*’) en de federale gerechtelijke instantie (‘*Bundesgerichtshof*’). Deze laatste is de hoogste instantie in de federale rechtspraak (Struijk, 2018, p. 496).
[91] § 100a (3) Sv.
[92] § 100b (3) Sv.
[93] § 100a (1) 1 Sv.
[94] § 100b (1) 1 Sv.

voorwaarden van de oorspronkelijke machtiging voor de bronintercepte nog steeds gelden.[95] In de wet is geen maximale periode genoemd dat deze bevoegdheid mag worden ingezet. Hetzelfde geldt voor het maximaal aantal verlengingen. De online doorzoeking kan maximaal één maand worden ingezet. De machtiging voor de inzet van de bevoegdheid kan steeds met één maand worden verlengd tot in eerste instantie een maximale periode van zes maanden. Wanneer de periode van zes maanden is bereikt, beslist het gerechtshof (*'des Oberlandesgericht'*) over eventuele verlenging van de inzet van de online doorzoeking. In de wet is niets vastgelegd over het maximum aantal verlengingen of een verdere maximale periode. Ook voor de online doorzoeking geldt dat de voorwaarden van de oorspronkelijke machtiging aanwezig moeten zijn, rekening houdend met de informatie die in de loop van het opsporingsonderzoek is verkregen.[96]

4.6 Formaliteiten

De rechter of rechtbank die een beslissing neemt over de inzet van de bevoegdheid, of over verlenging daarvan, motiveert de vereisten en belangrijkste overwegingen onderhevig aan diens beslissing. De rechter of rechtbank moet in het bijzonder in iedere individuele zaak het volgende vermelden: de specifieke feiten waarop de verdenking is gebaseerd en de belangrijkste overwegingen omtrent de noodzakelijkheid en proportionaliteit van de inzet van de bevoegdheid.[97] Wanneer niet meer kan worden voldaan aan de voorwaarden voor de inzet, wordt de inzet van de bevoegdheid direct beëindigd. De rechtbank wordt daarvan op de hoogte gebracht.[98] Verder dient de machtiging van de rechter of rechtbank schriftelijk te worden verleend.[99] In de schriftelijke machtiging moet het volgende worden opgenomen:

1 Voor zover bekend de naam en het adres van de verdachte tegen wie de bevoegdheid is gericht.
2 Het vermeende misdrijf.
3 Het type, de omvang, de duur en de eindtijd van de inzet van de bevoegdheid.
4 Het soort informatie dat moet worden verzameld en de relevantie daarvan voor het onderzoek.
5 Een zo nauwkeurig mogelijke beschrijving van het geautomatiseerd werk waaruit gegevens moeten worden verzameld als het gaat om de inzet van de bevoegdheid uit § 100a (1) tweede en derde zin Sv of § 100b Sv.[100]

De inzet van beide bevoegdheden is, naast het vermoeden dat de verdachte een (zeer) ernstige vorm van criminaliteit heeft gepleegd, alleen toegestaan als het misdrijf in de individuele zaak ook (zeer) ernstig is.[101] Ook moeten andere maatregelen voor het vaststellen van de feiten of het bepalen van de verblijfplaats van de verdachte geen of minder kans van slagen hebben (het subsidiariteitsbeginsel) (Lindemann & Van Toor, 2018, p. 381).[102] In het geval van bronintercepte betekent dit bijvoorbeeld dat de inzet van de bevoegdheid pas toelaatbaar is, als de traditionele

95 § 100e (1) Sv.
96 § 100e (2) Sv.
97 § 100e (4) Sv.
98 § 100e (5) Sv.
99 § 100e (3) Sv.
100 § 100e (3) Sv.
101 Lindeman & Van Toor (2018, p. 381) geven het voorbeeld van een gedwongen tongzoen die bestraft kan worden als verkrachting. Verkrachting is een ernstig misdrijf, maar gezegd zou kunnen worden dat sommige handelingen die als verkrachting gekwalificeerd kunnen worden, in de praktijk niet gezien zullen worden al een ernstig misdrijf.
102 § 100a (1) en § 100b (1) Sv.

interceptiebevoegdheid niet kan worden gebruikt (Singelnstein & Derin, 2017, p. 2648).

Tot slot dienen opsporingsinstanties rekening te houden met de persoonlijke levenssfeer van de verdachte (‘*Kernbereich privater Lebensgestaltung*’). In § 100d Sv staat dat bronintercepție en de online doorzoeking niet mogen worden ingezet wanneer er aanwijzingen zijn dat met de inzet van de bevoegdheid enkel informatie wordt verkregen uit de kern van de persoonlijke levenssfeer van een verdachte. Wanneer tijdens de inzet van een van de bevoegdheden dergelijke bevindingen worden gedaan, moeten deze onmiddellijk worden verwijderd. Bovendien moeten bij de inzet van een online doorzoeking technische maatregelen worden genomen om ervoor te zorgen dat gegevens uit de persoonlijke levenssfeer van een verdachte niet kunnen worden verzameld.[103]

4.7 Technische hulpmiddelen

Zowel in § 100a (1) Sv als in § 100b (1) Sv is geregeld dat opsporingsinstanties gebruik kunnen maken van technische hulpmiddelen. De BKA heeft voor bron-interceptie zowel zelf ontwikkelde als commerciële software tot haar beschikking. Deze software wordt pas vrijgegeven als een uitgebreide testprocedure is doorlopen en als vastgesteld is dat de software voldoet aan de wettelijke vereisten en aan de SLB-richtlijn (‘*Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung*’). In de SLB-richtlijn staan doelen en maatregelen geformuleerd waaraan de gebruikte software zou moeten voldoen. Verder vindt, afhankelijk van operationele vereisten, continue ontwikkeling plaats van de software. Ook voor de online doorzoeking beschikt de BKA over software (BKA, z.d.). Het is niet duidelijk of het daarbij ook gaat om zowel zelf ontwikkelde als commerciële software.

In principe mogen alle technische hulpmiddelen worden gebruik zolang zij aan de wettelijke en constitutionele voorwaarden voldoen.[104] In de praktijk zal de politie ervoor moeten zorgen dat de gebruikte middelen aan de voorwaarden voldoen. De SLB-richtlijn is een interne richtlijn voor de opsporingsfunctionarissen en heeft verder geen bindende wettelijke status (persoonlijke communicatie, 23 mei 2023). De eerste SLB-richtlijn is in 2012 opgesteld door de veiligheidsautoriteiten van zowel de federale overheid als van de deelstaten. Op 2 oktober 2012 hebben twee werkgroepen van de Conferentie van ministers van Binnenlandse Zaken (‘*Innenministerkonferenz*’) kennis-genomen van de voorgestelde richtlijn. Zij hebben zowel de federale overheid als de deelstaten aanbevolen om de richtlijn te gebruiken als basis voor het aanschaffen en ontwikkelen van interceptiesoftware. Vanwege de korte innovatiecycli die moderne informatietechnologiesystemen en hun software doorgaans kennen en omdat in 2017 het Duitse Wetboek van Strafvordering is aangepast, is de richtlijn uit 2012 aangepast (BKA, 2018, p. 1). De oorspronkelijke richtlijn, die zich richtte op onderschepping en pc-platforms, bevatte zeer specifieke technische specificaties. De nieuwste versie van de richtlijn is op een meer open wijze geformuleerd. Dat betekent dat niet zozeer technieken worden gespecificeerd, maar in plaats daarvan te behalen doelen.

[103] Zie § 100d (1) (2) (3) Sv.

[104] De wettelijke voorwaarden zijn te vinden in §100a (5). De constitutionele voorwaarden volgen uit jurisprudentie van het federaal constitutioneel hof (BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07). Heimelijke infiltratie van een geautomatiseerd werk moet altijd gebaseerd zijn op een gerechtelijk bevel en een wet die binnendringingen mogelijk maakt moet bepalingen bevatten om de persoonlijke levenssfeer te beschermen (persoonlijke communicatie, 7 juni 2023).

Bovendien geldt de richtlijn niet alleen voor bronintercepte, maar ook voor de online doorzoeking (BKA, z.d.). Het is de bedoeling dat de richtlijn met enige regelmaat wordt bijgewerkt. De meest recente versie is van 5 oktober 2018 (BKA, 2018). In de richtlijn blijkt dat de software die wordt gebruikt voor beide bevoegdheden uit een aantal componenten bestaat die samen functioneren als één systeem:

1 De ophaalsoftware (‘*Ausleitungssoftware*’) wordt op het geautomatiseerd werk van de verdachte geïnstalleerd en zorgt ervoor dat gegevens worden verzameld en worden doorgestuurd naar degene die uitvoering geeft aan de bevoegdheid.
2 De registratie- en controle-eenheid (‘*Steuer- und Aufzeichnungseinheit*’) wordt door uitvoerende actoren gebruikt om de ophaalsoftware aan te sturen, om de gegevens uit het besluit van de rechtbank op te nemen en om alle activiteiten te loggen.
3 De netwerkverbinding (‘*Netzwerkverbindung*’) stuurt de communicatie van het geautomatiseerd werk van de verdachte naar de registratie- en controle-eenheid van de opsporingsinstanties, en weer terug (BKA, 2018, p. 2).

4.7.1 ZITiS

In Duitsland bestaat sinds 2017 een organisatie die opsporingsinstanties kan ondersteunen bij bronintercepte en de online doorzoeking. Deze organisatie, genaamd ‘*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*‘ (hierna ZITiS), valt onder het Duitse ministerie van Binnenlandse Zaken (‘*Bundesministerium des Innern und für Heimat*)’, maar kan zelf geen opsporingsbevoegdheden inzetten en is niet betrokken bij het gebruik van technische hulpmiddelen.[105] De taak van ZITiS is om federale veiligheidsdiensten te ondersteunen en te adviseren bij beveiligingstaken op het gebied van informatietechnologie. Daarnaast vervult zij een rol rondom (onderzoek naar en de ontwikkeling van) producten zoals technische hulpmiddelen voor de federale veiligheidsdiensten.[106] Uit een interview blijkt dat ZITiS bijvoorbeeld op verzoek van de politie marktonderzoek kan uitvoeren (welke technische hulpmiddelen zijn er op de markt en wat is de kwaliteit ervan?). Ook kijkt ZITiS of technische hulpmiddelen voor bronintercepte of de online doorzoeking binnen de Duitse wetgeving passen. De aanbevelingen van ZITiS zijn wettelijk gezien geen certificering, maar het kan de politie wel helpen bij de aanschaf van een technisch hulpmiddel. De eindbeslissing over de aanschaf van een technisch hulpmiddel ligt bij de politie zelf. Zij moet zelf het technisch hulpmiddel aanschaffen. Ook is ZITiS recentelijk gestart met het ontwikkelen van eigen technische hulpmiddelen voor de hackbevoegdheid, zo blijkt uit een interview.

4.8 Waarborgen

4.8.1 Technische vereisten

Hoewel in de wet voor zover bekend niets is vastgelegd over het soort technische hulpmiddelen dat opsporingsinstanties mogen gebruiken, is wel een aantal vereisten opgenomen waaraan een technisch hulpmiddel moet voldoen. Deze vereisten gelden zowel voor bronintercepte als voor de online doorzoeking. In § 100a (5) Sv staan de vereisten beschreven waaraan technische hulpmiddelen, gebruikt voor bronintercepte, moeten voldoen. Het gaat om de volgende vereisten:

[105] Artikel 1 uit het Instellingsbesluit van ZITiS, de *'Erlass über die Errichtung der Zentralen Stelle für Informationstechniek im Sicherheitsbereich'* (hierna Instellingsbesluit) (Bundesministerium des Innern, 2017).
[106] Artikel 2 van het Instellingsbesluit. Zie ook: ZITiS (z.d.).

1 Een technisch hulpmiddel moet zo worden ingesteld dat het alleen lopende communicatie[107] of de inhoud en de omstandigheden van communicatie[108] opneemt.
2 Technische hulpmiddelen mogen alleen wijzigingen aanbrengen aan het geautomatiseerd werk van de betrokken persoon die essentieel zijn voor de dataverzameling.
3 De aangebrachte wijzigingen moeten, indien technisch mogelijk, na beëindiging van de inzet van de bevoegdheid automatisch ongedaan worden gemaakt.
4 Verder moeten technische hulpmiddelen, volgens de stand van de techniek, bescherming bieden tegen ongeoorloofd gebruik door derden. Gekopieerde gegevens moeten, volgens de stand van de techniek, worden beschermd tegen wijziging, ongeoorloofde verwijdering en ongeoorloofde toegang door derden.

§ 100b (4) Sv regelt dat deze vereisten ook gelden voor technische hulpmiddelen die worden gebruikt bij een online doorzoeking met uitzondering van het eerstgenoemde vereiste.

Naast deze wettelijke vereisten zijn in de SLB-richtlijn diverse aspecten opgenomen die ervoor moeten zorgen dat de ontwikkeling, de inkoop en het gebruik van de software binnen een uniform kader plaatsvinden (BKA, 2018). De in de richtlijn opgenomen onderwerpen zijn voor een groot gedeelte te relateren aan de in de wet genoemde vereisten. De richtlijn is onderverdeeld in de volgende onderwerpen: beschermingsdoelen en veiligheidsmaatregelen, werkprocessen en procedures, leveranciers en testbeleid. Ook wordt in de richtlijn een framework gepresenteerd aan de hand waarvan naar de ontwikkeling en het gebruik van software wordt gekeken. Daarbij gaat het om risicoanalyses en IT-securityconcepten. Om beide bevoegdheden (broninterceptie en online doorzoeking) in te kunnen zetten, dienen speciale beveiligingsconcepten te worden ontwikkeld, aldus de SLB-richtlijn. Zowel leveranciers van software als gebruikers van de software dienen zich aan deze concepten te conformeren. Onderdeel van een IT-beveiligingsconcept is het maken van een risicoanalyse. Daarin zou onder andere aandacht moeten zijn voor bedreigingen die het IT-proces kunnen beïnvloeden en bestaande restrisico's. Objecten die risico lopen (denk aan systeemcomponenten zoals hard- en software, applicaties, organisatorische of personele aangelegenheden) dienen te worden beschreven en te worden geëvalueerd. De resultaten van de risicoanalyse, de vaststelling van de beschermingsbehoeften en de daaruit voortvloeiende gevolgen en de uitvoering ervan, worden vastgelegd in het IT-beveiligingsconcept. Dit beveiligingsconcept moet passende, actuele beveiligingsmaatregelen naar de stand van de techniek bevatten (BKA, 2018, p. 4).

Beschermingsdoelen en veiligheidsmaatregelen
In de SLB-richtlijn worden de volgende beschermingsdoelen genoemd: vertrouwelijkheid, integriteit/authenticiteit en beschikbaarheid van gegevens.[109] Vertrouwelijkheid betekent dat geen ongeautoriseerde toegang plaatsvindt. Met integriteit en authenticiteit wordt bedoeld dat verzamelde gegevens zijn beschermd tegen wijzigingen en dat gegevenswijzigingen herleidbaar zijn. De overdracht van communicatie mag uitsluitend plaatsvinden tussen de ophaalsoftware op het

[107] § 100a (1) tweede zin Sv.
[108] § 100a (1) derde zin Sv.
[109] Dit zijn bekende begrippen die in de informatiebeveiliging worden gebruikt, de zogenoemde CIA-driehoek. Confidentiality (vertouwelijkheid), Integrity (integriteit) and Availability (beschikbaarheid). In het Nederlandse Besluit worden andere termen gebruikt in het kader van de kwaliteit van gegevens, namelijk: betrouwbaarheid, integriteit en herleidbaarheid. De beschikbaarheid is geen onderwerp in het besluit. Integriteit en vertrouwelijkheid vertonen overeenkomsten met de begrippen betrouwbaarheid, integriteit en herleidbaarheid.

geautomatiseerd werk van de verdachte en de registratie- en controle-eenheid van de uitvoerende instantie. Beschikbaarheid tot slot betekent dat maatregelen genomen moeten worden om het verlies van de opgehaalde gegevens tegen te gaan en om het gehele geautomatiseerd werk te beschermen tegen verstoringen (BKA, 2018, p. 3). In de richtlijn wordt opgemerkt dat (technische) maatregelen nodig zijn, die voldoen aan de stand van de techniek, om deze doelen te kunnen realiseren. Het gaat bijvoorbeeld om het gebruik van cryptografische methodes (BKA, 2018, p. 3-4).

Werkprocessen en procedures
De uitvoering van beide bevoegdheden gebeurt volgens de wettelijke en organisatorische kaders èn de concepten voor organisatieprocessen en kwaliteitsborging die gezamenlijk door de federale en deelstatelijke veiligheidsinstanties zijn ontwikkeld. Het doel daarvan is dat er overkoepelende standaarden ontstaan die de uitvoering van beide bevoegdheden zo optimaal mogelijk laten verlopen en het risico van ontdekking tot een minimum beperken. Daarmee wordt, zo is de verwachting, een gestandaardiseerd en rechtmatig gebruik van software gewaarborgd (BKA, 2018, p. 5).

De geformuleerde processen en procedures hebben betrekking op de volgende thema's: de reikwijdte van de toegang tot gegevens zoals genoemd in het bevel, toegangsrechten en rolverdeling, en wijzigingen aan het geautomatiseerd werk van de verdachte. Daarnaast hebben deze betrekking op de bescherming van derden die niet direct onderwerp van onderzoek zijn, updates en bescherming tegen openbaarmaking en herleidbaarheid.

Reikwijdte toegang tot gegevens en rollen en rechten
Wat betreft de toegang tot verzamelde gegevens dienen passende technische en organisatorische veiligheidsmaatregelen genomen te worden die ervoor zorgen dat degene die de bevoegdheid uitvoert alleen kennis kan nemen van de inhoud die onder het bevel valt. Dit dient geregistreerd of gedocumenteerd te worden. De persoonlijke levenssfeer wordt in het bijzonder beschermd. De processen zijn in overeenstemming met de betreffende wettelijke kaders (BKA, 2018, p. 5).

In de richtlijn staat verder beschreven dat rollen en toegangsrechten op zo'n manier dienen te zijn vastgelegd dat gebruikers alleen toegangsrechten hebben die nodig zijn om hun rol uit te kunnen voeren. Dit betekent dat toegangsbescherming in lijn met het gegevensbeschermingsrecht, de bijbehorende registratie en in het bijzonder de naleving van de regelgeving ter bescherming van de persoonlijke levenssfeer gewaarborgd moet worden. De uitvoerende instantie is verantwoordelijk voor de concrete invulling van het toegangsrechten- en rollenconcept in overeenstemming met de organisatorische en juridische randvoorwaarden (BKA, 2018, p. 5).

Wijzigingen geautomatiseerd werk verdachte
Met betrekking tot het aanbrengen van wijzigingen aan het geautomatiseerd werk van de verdachte staat in de richtlijn beschreven dat dit geautomatiseerd werk niet meer dan noodzakelijk mag worden aangetast. Het is verder niet de bedoeling dat beveiligingsmaatregelen die het geautomatiseerd werk van de verdachte tegen toegang van buitenaf beschermen langer beperkt worden dan noodzakelijk. Daarnaast moet de *interface* waarmee de ophaalsoftware gegevens aan de gebruikers ter beschikking stelt, door beveiligingsmaatregelen tegen ongeoorloofd gebruik worden beschermd. Voorafgaand aan het gebruik van de software dient gecontroleerd en gedocumenteerd te worden dat de aantasting van het geautomatiseerd werk van de verdachte door de software tot het onvermijdelijke minimum beperkt blijft (BKA, 2018, p. 5).

Op het moment dat het verzamelen van gegevens is afgerond, dient de software onmiddellijk te worden verwijderd. Mochten er in het kader van de bevoegdheid wijzigingen hebben plaatsgevonden aan het geautomatiseerd werk van de verdachte, dan dienen deze, voor zover technisch mogelijk, hersteld te worden. De software moet hiervoor over passende functies beschikken zodat het herstel ook realiseerbaar is wanneer het geautomatiseerd werk van de verdachte niet meer door de registratie- en controle-eenheid bereikbaar is (BKA, 2018, p. 6).

Bescherming van derden en updates
De ophaalsoftware mag alleen worden ingezet op het geautomatiseerd werk dat in het bevel wordt genoemd. Daarom is het van belang om dit geautomatiseerd werk zo nauwkeurig mogelijk te identificeren. Mocht de ophaalsoftware worden gestart op een ander geautomatiseerd werk dan het geautomatiseerd werk van de verdachte, dan dient ervoor gezorgd te worden dat geen gegevens van dat geautomatiseerd werk worden overgedragen behalve de gegevens die nodig zijn in het kader van de identificatie van het geautomatiseerd werk van de verdachte. Ook moet, voor zover technisch mogelijk, de software direct worden verwijderd en moeten eventueel doorgevoerde wijzigingen worden hersteld (BKA, 2018, p. 6).

Voor het verzenden van updates gelden specificaties en maatregelen die de betrouwbaarheid, integriteit/authenticiteit en herleidbaarheid van gegevens waarborgen. Dit garandeert dat updates van de software uitsluitend via de registratie- en controle-eenheid van de uitvoerende instantie worden uitgevoerd. Met behulp van registratie en documentatie moet kunnen worden nagegaan wanneer en welke updates zijn uitgevoerd. Voor zover technisch mogelijk moet door passende beveiligingsmaatregelen worden uitgesloten dat de maatregel ontdekt en naar de uitvoerende instantie herleid kan worden. In het bijzonder moet de software worden beschermd tegen *reverse engineering*. Mochten zich bij de software of bij de registratie- en controle-eenheid veiligheidsproblemen voordoen, dan is de aanbieder van de software verplicht om deze problemen direct te verhelpen en passende updates te verzorgen. Uitvoerende instanties dienen deze updates direct te installeren, overeenkomstig het IT-beveiligingsconcept (BKA, 2018, p. 6-7).

Herleidbaarheid
In de richtlijn wordt beschreven dat de herleidbaarheid en authenticiteit van de gegevens belangrijk zijn. Omdat gegevens worden gebruikt voor wetshandhavings- en veiligheidsdoeleinden is het nodig dat volledig inzicht kan worden gegeven in de verzameling, evaluatie en verdere verwerking van de gegevens door de uitvoerende instantie.

Registratie en documentatie moeten ervoor zorgen dat de rechtmatigheid van de gegevensverzameling en de wijze waarop gegevens zijn verwerkt, kunnen worden gecontroleerd. Ook moeten registratie en documentatie ertoe leiden dat de bescherming van grondrechten wordt gewaarborgd, maar ook dat de integriteit (bruikbaarheid in rechtszaken) van de opgehaalde gegevens wordt gegarandeerd. Verder helpt het vastleggen vooral om aan te tonen dat gegevens daadwerkelijk afkomstig zijn van het geautomatiseerd werk van de verdachte, dat ze volledig zijn en dat ze niet gemanipuleerd zijn. Om de herleidbaarheid te waarborgen dient de gebruikte software te worden gearchiveerd. De duur van de opslag van protocolgegevens is afhankelijk van de wettelijke voorschriften van de federale regering en van de verschillende deelstaten.

Softwareleveranciers
In de richtlijn staat beschreven dat leveranciers (*'Anbieter'*) van software zorgvuldig geselecteerd dienen te worden. Voor binnenlandse leveranciers zou het federale ministerie van Economische Zaken en Technologie een beveiligingsrapport moeten opmaken. Voor buitenlandse leveranciers dient een passende procedure te worden gezocht (BKA, 2018, p. 7). Leveranciers dienen te garanderen dat zij zich houden aan de voorwaarden en de condities die volgen uit het wettelijk kader en de SLB-richtlijn. Verder dienen zij het volgende te verzekeren:

1 Er wordt gehandeld in lijn met veilige softwareontwikkeling naar de stand van de techniek.
2 Alleen geautoriseerde personen hebben fysieke toegang, toegang tot logging en toegang tot de ontwikkelomgeving.
3 Externe componenten zoals '*software libraries*'[110] worden aangeschaft bij geverifieerde bronnen en worden voorafgaand aan het gebruik getest wat betreft hun beveiligingseigenschappen.
4 Instanties die de software gebruiken worden direct op de hoogte gesteld van beveiligingsincidenten, geïdentificeerde beveiligingstekortkomingen of andere gebeurtenissen die een veilige, wettelijke en juiste uitvoering van de bevoegdheden in gevaar brengen.

Toetsing van deze punten vindt plaats door de instantie die de software gebruikt of een andere door deze aangewezen instantie, bijvoorbeeld als onderdeel van een aanbestedingsprocedure (BKA, 2018, p. 7-8).

Testen en aanschaf
Goedkeuring van software gebeurt op basis van een gedefinieerde testprocedure waarvan de resultaten worden vastgelegd als onderdeel van het totale acceptatie-proces. Voorafgaand aan iedere toepassing, toetst de uitvoerende instantie of in het concrete geval aan de wettelijke voorschriften is voldaan, bijvoorbeeld wat betreft de gebruikte functies van de software. De resultaten van deze toetsing worden gedocumenteerd (BKA, 2018, p. 8). Verder blijkt uit één van de interviews dat soms ook onafhankelijke organisaties, zoals TÜV en de Fraunhofer-Gesellschaft, kunnen worden gevraagd om technische hulpmiddelen te keuren.[111] Wat hun rol precies is, is in dit onderzoek niet duidelijk geworden.

4.8.2 Verslaglegging en dossier

Naast de zojuist genoemde maatregelen zijn er nog andere maatregelen die relevant zijn voor de (controle op de) kwaliteit van de verzamelde gegevens, zoals de wijze waarop verslaglegging plaatsvindt, dossiervorming en de notificatieplicht.
Iedere keer dat een technisch hulpmiddel wordt gebruikt voor broninterceptie of voor een online doorzoeking, moeten opsporingsinstanties daar verslag van doen.[112] Het gaat om een verplichting tot logging aan de hand waarvan gecontroleerd kan worden of opsporingsautoriteiten de bevoegdheid op een rechtmatige manier hebben ingezet. De volgende informatie dient te worden gegeven: (1) de benaming van het technisch hulpmiddel en het tijdstip van het gebruik; (2) informatie over de identificatie van het geautomatiseerd werk en over de aangebrachte niet tijdelijke wijzigingen; (3) informatie aan de hand waarvan de verzamelde gegevens kunnen worden vastgelegd; en

[110] Een *software library*, ofwel softwarebibliotheek, is een verzameling van gegevens en programmeercodes die kunnen worden gebruikt om software(-applicaties) te ontwikkelen (Techopedia, 2016).
[111] Ook twee mediaberichten maken melding van de rol van TÜV (Meister, 2018; Flade, 2018).
[112] § 100a (6) Sv & § 100b (4) Sv.

(4) de eenheid die de bevoegdheid uitvoert.[113] Naast verslaglegging met betrekking tot het gebruik van het technisch hulpmiddel dient het Openbaar Ministerie de genomen beslissingen en de documentatie rondom de online doorzoeking te bewaren. Deze informatie wordt aan het dossier toegevoegd als aan de notificatieplicht is voldaan.[114] Voor persoonsgegevens (*'Personenbezogene Daten'*) gelden andere regels.[115]

Op basis van § 101 (4) Sv moeten personen ten aanzien van wie broninterceptie of de online doorzoeking is ingezet, op de hoogte worden gebracht dat opsporingsinstanties deze bevoegdheden hebben ingezet. Die kennisgeving moet zo snel mogelijk plaatsvinden. Kennisgeving kan worden uitgesteld, bijvoorbeeld als het doel van het onderzoek, het leven, de fysieke integriteit en de persoonlijke vrijheid van een persoon of belangrijke vermogensbestanddelen in gevaar komen.[116] Indien kennisgeving wordt uitgesteld en niet binnen twaalf maanden na voltooiing van de inzet van de bevoegdheid plaatsvindt, zal de bevoegde rechtbank over eventueel verder uitstel en over de duur ervan beslissen. Ook kan de bevoegde rechtbank de beslissing nemen dat notificatie geheel achterwege wordt gelaten.[117]

4.8.3 Extern toezicht

Er zijn voor zover bekend geen externe toezichthouders in Duitsland die toezien op de inzet van de hackbevoegdheid.

4.9 Jurisprudentie

De deelstaten en de Procureur-Generaal (*'Generalbundesanwalt'*) moeten jaarlijks een rapport uitbrengen aan het Federale Bureau voor Justitie (*'Bundesamt für Justiz'*) over de inzet van (bron-)interceptie van telecommunicatie en de online doorzoeking. Het Federale Bureau voor Justitie maakt van deze rapporten een landelijk overzicht en publiceert ze online.[118] De volgende informatie dient voor beide bevoegdheden in het jaarlijks overzicht te worden vastgelegd:

1 Het aantal zaken waarin de bevoegdheid van § 100a (1) Sv (traditionele interceptiebevoegdheid) of § 100b (1) Sv is bevolen.
2 Het aantal bevelen. Een onderscheid wordt gemaakt tussen eerste bevelen en verlengingsbevelen.
3 Het onderliggende misdrijf op grond waarvan de bevoegdheid is ingezet.
4 Het aantal zaken waarin een ingreep in het geautomatiseerd werk op grond van § 100a (1) tweede en derde zin Sv (broninterceptie) is bevolen en daadwerkelijk is uitgevoerd. In het geval van de online doorzoeking, het aantal zaken waarin daadwerkelijk een ingreep in het geautomatiseerd werk van de verdachte is uitgevoerd.[119]

In 2020 is de broninterceptie veertien keer uitgevoerd. De online doorzoeking is in 2020 uiteindelijk acht keer ingezet (Bundesamt für Justiz, z.d.).

[113] § 100a (6) Sv.
[114] § 101 (2) Sv.
[115] § 101 (3) (8) Sv.
[116] § 101 (5) Sv.
[117] § 101 (6) (7) Sv.
[118] § 101b (1) Sv. Zie: Bundesamt für Justiz (z.d.).
[119] § 101b (2) (3) Sv.

Voor zover uit interviews bekend is er op dit moment geen jurisprudentie beschikbaar van rechtszaken waarin de kwaliteit van de verkregen gegevens met betrekking tot een individuele zaak ter sprake is gekomen.

4.10 Tot slot

In Duitsland kunnen opsporingsdiensten op basis van twee wetsartikelen hacken. Bronінterceptie (§ 100a (1) tweede en derde zin Sv) maakt het voor opsporingsinstanties mogelijk om telecommunicatie bij de bron te onderscheppen. Met behulp van de online doorzoeking (§ 100b (1) Sv) mogen opsporingsinstanties toegang krijgen tot in principe alle gegevens die in een geautomatiseerd werk van een verdachte staan opgeslagen. Met deze tweede bevoegdheid maken opsporingsdiensten een ingrijpendere inbreuk op het privéleven van verdachten. Om die reden gelden strengere voorwaarden voor de inzet van de online doorzoeking. Op basis van de zojuist genoemde twee wetsartikelen mogen opsporingsinstanties geen camera of microfoon aanzetten om video- of geluidsopnames te maken. Ook mogen geen gegevens worden gewijzigd.

Bij de inzet van zowel bronінterceptie als van de online doorzoeking kunnen technische hulpmiddelen worden gebruikt. In het Duitse Wetboek van Strafvordering zijn enkele waarborgen opgenomen die de kwaliteit van de verzamelde gegevens zoveel mogelijk moeten garanderen. Ook in een door de veiligheidsautoriteiten opgestelde SLB-richtlijn worden waarborgen beschreven, deels overlappend met de wettelijke vereisten. In deze richtlijn wordt overigens (bewust) niet aangegeven hoe die waarborgen in de praktijk gerealiseerd dienen te worden. De SLB-richtlijn geldt voor zowel zelf ontwikkelde tools als voor software gecreëerd door leveranciers. Opvallend aan de Duitse waarborgen is dat deze betrekking hebben op de fase voorafgaand aan, tijdens en na afloop van een inzet. Verder valt op dat de waarborgen veelal betrekking hebben op de integriteit en de betrouwbaarheid van de verzamelde gegevens. Minder aandacht is er voor de herleidbaarheid van de gegevens.

4.10.1 Voorafgaand aan een inzet

Zowel in de wettelijke regeling als in de SLB-richtlijn komt naar voren dat een technisch hulpmiddel niet meer mag opnemen of wijzigen aan een geautomatiseerd werk dan nodig. Gegevens dienen te worden beschermd tegen wijziging, verwijdering en ongeautoriseerde toegang door derden. In de SLB-richtlijn staat verder nog genoemd dat eventuele wijzigingen herleidbaar dienen te zijn en dat de communicatieoverdracht plaats moet vinden tussen de ophaalsoftware op het geautomatiseerd werk van de verdachte en de registratie-en controle-eenheid van de uitvoerende instantie.
Naast de eisen die worden gesteld aan een technisch hulpmiddel, bestaat in Duitsland een testprocedure voor de goedkeuring van software. Het is niet duidelijk geworden wie deze testen uitvoert en wie bijvoorbeeld kijkt of een hulpmiddel aan de SLB-richtlijnen voldoet. Duitsland lijkt geen instantie te kennen die vergelijkbaar is met de Keuringsdienst in Nederland. Wel kent Duitsland de organisatie ZITiS. Zij speelt een rol rondom (onderzoek naar en de ontwikkeling van) technische hulpmiddelen door bijvoorbeeld marktonderzoek uit te voeren en te kijken of een technisch hulpmiddel binnen de Duitse wetgeving valt.

4.10.2 Tijdens en na afloop van een inzet

Het Duitse Wetboek van Strafvordering en de SLB-richtlijn regelen dat opsporingsinstanties informatie dienen vast te leggen (logging en documentatie), indien een technisch hulpmiddel wordt gebruikt voor het verzamelen van gegevens. Bijvoorbeeld informatie aan de hand waarvan de verzamelde gegevens kunnen worden vastgesteld. Logging en documentatie moeten er onder andere voor zorgen dat de integriteit van de verzamelde gegevens gewaarborgd wordt: dat ze inderdaad afkomstig zijn van het geautomatiseerd werk van de verdachte, dat ze volledig zijn en dat de gegevens niet zijn gemanipuleerd. De SLB-richtlijn kent daarnaast nog twee andere waarborgen met betrekking tot de integriteit van gegevens tijdens de inzet van de bevoegdheden. Ten eerste krijgen alleen medewerkers die de bevoegdheid uitvoeren toegang tot de verzamelde gegevens. Dat moet worden gedocumenteerd. Ten tweede krijgen medewerkers alleen toegangsrechten die noodzakelijk zijn voor de uitvoering van hun rol. Voor de herleidbaarheid van de gegevens moet de gebruikte software gearchiveerd worden.

Na afloop van de inzet van bronintercepte of van de online doorzoeking is er in Duitsland een notificatieplicht. Dat betekent dat personen ten aanzien van wie de hackbevoegdheid is ingezet, in principe daarvan op de hoogte worden gebracht. Indien een zaak ter zitting komt, kan de kwaliteit van de verzamelde gegevens ter discussie worden gesteld aan de hand van de informatie die zij terugvinden in het dossier. Het zal de vraag zijn in hoeverre die informatie voldoende aanknopingspunten biedt om de kwaliteit van de gegevens te beoordelen.

5 Frankrijk

Dit hoofdstuk is gecontroleerd op feitelijke onjuistheden door twee juristen uit Frankrijk. Deze personen vonden het niet nodig bij naam te worden genoemd.

5.1 Wettelijke regeling

Op 14 maart 2011 wordt een bevoegdheid voor de politie geïntroduceerd zodat zij computergegevens mag vastleggen (‘*captation de données informatiques’*).[120] De bevoegdheid maakt het voor de politie mogelijk om heimelijk op afstand een geautomatiseerd werk[121] binnen te dringen. In het kader van de aanpak van georganiseerde criminaliteit en terrorisme is de reikwijdte van de bevoegdheid verschillende keren uitgebreid, namelijk in november 2014, augustus 2015 en juni 2016 (Ministère de la Justice, 2019, p. 1).[122] Op 23 maart 2019 is de wet voor het laatst gewijzigd. Er is een gemeenschappelijk kader voor drie bijzondere opsporingsbevoegdheden gecreëerd: het gebruik van de IMSI-catcher, interceptie van beeld en geluid en het vastleggen van computergegevens.[123] Op basis van deze wet wordt het vastleggen van computergegevens door een drietal artikelen in het Wetboek van Strafvordering (‘*Code de procédure pénale')* gereguleerd: artikel 706-95-11 Sv, artikel 706-102-5 Sv en artikel 15-1-6 Sv.

Het vastleggen van computergegevens is in artikel 706-102-1 Sv als volgt gedefinieerd: “met behulp van het inzetten van een technisch hulpmiddel, zonder toestemming van de betrokken partijen, toegang krijgen tot computergegevens, deze opnemen, opslaan en overdragen, zoals ze zijn opgeslagen in een computersysteem, zoals ze worden weergegeven op een scherm voor de gebruiker van een geautomatiseerd werk, zoals dat hij ze daar invoert door karakters in te voeren of zoals ze worden ontvangen en uitgezonden door audiovisuele randapparatuur”.[124]

Op basis van de bevoegdheid mag de politie zowel opgeslagen als stromende gegevens vastleggen. Dit betekent dat opgeslagen gegevens zoals foto's, video's en chats mogen worden geraadpleegd. Daarnaast mag de bevoegdheid ook worden ingezet om ‘live’ audio en video te onderscheppen (Ministère de la Justice, 2019, p. 1-2). In de interviews komt naar voren dat er discussie is over de reikwijdte van de bevoegdheid. Er is een specifieke surveillance bevoegdheid die het mogelijk maakt heimelijk een microfoon of camera te plaatsen,[125] maar in de wet wordt nergens expliciet vermeld of dit ook mogelijk is met de bevoegdheid die het vastleggen van

[120] Deze bevoegdheid wordt geïntroduceerd in de zogenaamde LOPPSI wet van 14 maart 2011 (wet nr. 2011-267), wat vrijuit staat voor de Wet begeleiding en programmering voor de binnenlandse veiligheid (‘*Loi d’orientation et de programmation pour la sécurité intérieure’*).

[121] In Frankrijk wordt gesproken van een geautomatiseerd gegevensverwerkingssysteem (‘*Système de traitement automatisé de données’ of ‘STAD’*). Dit begrip kent geen wettelijke definitie, maar uit jurisprudentie blijkt dat het een breed begrip is. Het kan gaan om zeer uiteenlopende systemen, zoals databeheerinfrastructuren, bankkaarten, bedrijfscomputersystemen en websites (Mattatia, 2015, p. 838).

[122] De wet van 13 november 2014 voegde de mogelijkheid toe om toegang te krijgen tot gegevens zoals ontvangen en uitgezonden door audiovisuele apparaten. De wet van 17 augustus 2015 breidde het toepassingsgebied uit tot misdrijven met betrekking tot economische delinquentie, handel in cultuurgoederen en illegale gokactiviteiten. De wet van 3 juni 2016 stond aanklagers toe om deze techniek te gebruiken, met toestemming van de rechter van vrijheid en detentie.

[123] Wet nr. 2019-222, 23 maart 2019, Programmering 2018-2022 en hervorming van justitie (‘*LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justic*e’).

[124] Zie ook Ministère de la Justice (2019).

[125] Artikel 706-96 Sv.

computergegevens mogelijk maakt. Een geïnterviewde van het Franse ministerie van justitie bevestigd dat het op dit moment niet mogelijk is om een microfoon of camera op afstand te activeren (persoonlijke communicatie, 13 juli 2023).

5.2 Bevoegde autoriteiten

Net als België kent Frankrijk twee soorten voorbereidend onderzoek: een opsporingsonderzoek en een gerechtelijk vooronderzoek (‘*information judiciaire*’). In beide type onderzoeken mag de politie de bevoegdheid inzetten om computergegevens vast te leggen. Per type onderzoek verschilt de procedure om de bevoegdheid in te zetten.

Het opsporingsonderzoek is onderverdeeld in twee fases: ‘*enquête flagrance*’ (flagrant onderzoek) en de ‘*enquête préliminaire*’ (het vooronderzoek, niet te verwarren met het gerechtelijk vooronderzoek). De *enquête flagrance* start naar aanleiding van heterdaadzaken of strafbare feiten die net hebben plaatsgevonden (Verrest, 2018, p. 181). In beginsel moet na acht dagen een *enquête préliminaire* of gerechtelijk vooronderzoek worden geopend.[126] Hoewel de politie veel vrijheid heeft om zelfstandig op te treden gedurende het opsporingsonderzoek, mag de bevoegdheid alleen worden ingezet na een machtiging van de rechter van vrijheid en detentie (‘*juge des libertés et de la détention*’) op verzoek van de officier van justitie.[127]

In de volgende gevallen kan de officier van justitie besluiten een gerechtelijk vooronderzoek te vorderen:
1 een gerechtelijk vooronderzoek is verplicht in geval van een zwaar misdrijf;[128]
2 de opening van een gerechtelijk vooronderzoek is noodzakelijk om de verdachte in voorlopige hechtenis te nemen;[129]
3 de opening van een gerechtelijk vooronderzoek is nodig omdat bepaalde onderzoeksbevoegdheden nodig zijn die aan de onderzoeksrechter zijn voorbehouden.

Op het moment dat de officier van justitie het gerechtelijk vooronderzoek vordert, wordt de leiding van het onderzoek overgedragen aan de onderzoeksrechter. De te onderzoeken strafbare feiten door de onderzoeksrechter worden ingekaderd door de vordering van de officier van justitie. Alleen met een nieuwe vordering van de officier van justitie mogen aanvullende feiten worden onderzocht (Verrest, 2018, p. 184). De onderzoeksrechter kan in zijn onderzoek, na consultatie van de officier van justitie, besluiten tot de inzet van het vastleggen van computergegevens.[130]

Artikel D15-1-6 Sv geeft een opsomming van instanties die gebruik mogen maken van de bevoegdheid. Samengevat gaat het om verschillende onderdelen van de politie, de inlichtingendienst en de rijkswacht (‘*Gendarmerie Nationale*’).[131] De daadwerkelijke technische uitvoering van de bevoegdheid ligt bij de nationale technische dienst voor gerechtelijke vastlegging (‘*Service technique national de captation judiciaire*’ (hierna STNCJ)). Deze dienst valt formeel onder het ministerie van Binnenlandse Zaken en is verantwoordelijk voor de centralisatie en implementatie van technische hulpmiddelen

[126] In het kader van waarheidsvinding voor misdrijven waarop een gevangenisstraf van vijf jaar of meer staat, kan de officier van justitie besluiten het te verlengen voor een periode van maximaal acht dagen.
[127] Artikel 706-95-12 Sv.
[128] Artikel 79 Sv.
[129] Artikel 143-1 Sv.
[130] Artikel 706-95-12 Sv.
[131] De Gendarmerie Nationale is vergelijkbaar met de Koninklijke Marechaussee (KMar).

voor het vastleggen van computergegevens. De STNCJ coördineert of voert – indien nodig – ook de operaties uit om de technische hulpmiddelen te installeren (Ministère de la Justice, 2019, p. 6). In paragraaf 5.8.2 wordt uitgebreider ingegaan op deze organisatie.

5.3 Tegen wie

In de Franse wet wordt alleen melding gemaakt van het type misdrijven waarvoor de bevoegdheid mag worden ingezet (zie paragraaf 5.4 voor een overzicht van deze misdrijven). Dit betekent dat het vastleggen van computergegevens in ieder geval mag worden ingezet op het geautomatiseerd werk van een verdachte van één van deze misdrijven. Het is onduidelijk in hoeverre – zoals in sommige andere landen – de bevoegdheid ook op geautomatiseerde werken van personen waarmee de verdachte communiceert, mag worden ingezet. Op basis van artikel 706-102-5 Sv wordt een aantal locaties van geheimhouders expliciet uitgesloten om de bevoegdheid in te zetten. Het gaat daarbij onder meer om het voertuig, kantoor of huis van senatoren, advocaten, magistraten en journalisten.[132]

5.4 Gevallen

Op basis van artikel 706-102-1 Sv mag de politie alleen computergegevens vastleggen bij misdrijven van terroristische aard,[133] georganiseerde criminaliteit[134] en zware economische criminaliteit.[135] Ten aanzien van misdrijven van georganiseerde criminaliteit betreft het een twintigtal misdrijven (en voorbereiding daarvan), beschreven in artikel 706-73 Sv. Het gaat daarbij onder meer om moord gelinkt aan georganiseerde criminaliteit, witwassen en drugshandel gelinkt aan georganiseerde criminaliteit.[136] Ten aanzien van zware economische criminaliteit gaat het om twaalf misdrijven genoemd in artikel 706-73-1, waaronder het in georganiseerd verband overgaan tot illegale tewerkstelling, witwassen van geld en het illegaal exploiteren van casino's.

5.5 Termijn

De termijn waarbinnen de politie de bevoegdheid mag inzetten is afhankelijk van het type onderzoek. In het kader van het opsporingsonderzoek mag de bevoegdheid maximaal één maand worden ingezet, en mag de inzet eenmaal met één maand worden verlengd. In het kader van het gerechtelijk vooronderzoek geldt een termijn van maximaal vier maanden. De inzet kan, onder dezelfde voorwaarden, steeds met maximaal vier maanden worden verlengd, waarbij de totale termijn van de inzet niet langer mag duren dan twee jaar.

[132] Artikel 706-102-5 Sv jo. 56-1, 56-2 , 56-3, 56-5 en 100-7 Sv.
[133] Het gaat hier om misdrijven en overtredingen die terroristische daden vormen bedoeld in de artikelen 421-1 tot 421-6 van het Franse Wetboek van Strafrecht (‘*Code pénal*’).
[134] Beide onder artikel 706-73 Sv.
[135] Artikel 706-73-1 Sv.
[136] Verrest (2018, p. 188) merkt op dat niet alle misdrijven genoemd in artikel 706-73 Sv in de delicts-omschrijving melding maken van georganiseerd verband of terrorisme. Dit geldt onder meer voor witwassen. Dit betekent dat de bevoegdheid ook voor het onderzoek naar dit soort feiten mag worden ingezet.

5.6 Formaliteiten

Zoals opgemerkt mag de bevoegdheid om computergegevens vast te leggen worden ingezet gedurende het opsporingsonderzoek en het gerechtelijk vooronderzoek. Tijdens het opsporingsonderzoek is een machtiging van de rechter van vrijheid en detentie nodig. Tijdens het gerechtelijk vooronderzoek geeft de onderzoeksrechter zelf – na consultatie van de officier van justitie – een machtiging af.

Voor beide type onderzoeken geldt dat de bevoegdheid alleen mag worden ingezet in het geval van de in paragraaf 5.4 genoemde misdrijven. In tegenstelling tot veel andere landen geldt in Frankrijk geen proportionaliteitsvereiste anders dan een noodzakelijkheidsvereiste (Ministère de la Justice, 2019, p. 5). De beslissing om de bevoegdheid te gebruiken moet zijn omkleed met een verwijzing naar 'feitelijke en juridische omstandigheden' die de noodzaak van de inzet aantonen (art. 706-95-13 Sv). Slechts de behoefte aan informatie in het onderzoek is niet genoeg om een inzet van de bevoegdheid te rechtvaardigen (Ministère de la Justice, 2019, p. 5). Op basis van artikel 706-102-3 Sv moeten de volgende elementen in het bevel zijn opgenomen:

- de aard van het misdrijf waarvoor de bevoegdheid wordt ingezet;
- de exacte locatie of gedetailleerde beschrijving van het geautomatiseerd werk;
- de termijn van de inzet.

Indien er een onmiddellijk risico is op verlies van bewijsmateriaal of ernstige schade aan personen of goederen, mag de onderzoeksrechter in een gerechtelijk voor-onderzoek, op basis van artikel 706-95-15 Sv, een machtiging afgeven zonder eerst advies in te winnen bij de officier van justitie. In de machtiging moeten de feitelijke omstandigheden zijn opgenomen die het dreigende risico aantonen. Gedurende het opsporingsonderzoek staat deze spoedprocedure niet open.

5.6.1 Gebruik technische hulpmiddelen

Voor het vastleggen van computergegevens kan gebruik worden gemaakt van technische hulpmiddelen. Om het technisch hulpmiddel te plaatsen kan zowel fysiek als op afstand toegang worden verkregen tot het geautomatiseerd werk.[137] De wijze van toegang bepaalt de machtiging(-en) die benodigd zijn.

Om een technisch hulpmiddel fysiek te plaatsen kan een ambtenaar worden gemachtigd om een voertuig, privé-plaats of een woning binnen te gaan zonder medeweten van de bewoner of de gebruiker. In artikel 706-102-5 Sv wordt onderscheid gemaakt tussen het binnentreden van deze locaties tijdens en na 'wettelijke uren'. Deze uren hebben betrekking op de tijdstippen die worden gehanteerd voor het doen van huiszoekingen. Op basis van artikel 59 Sv dienen deze tussen 6 uur 's ochtends en 21 uur 's avonds plaats te vinden. Voor het fysiek plaatsen van een technisch hulpmiddel kunnen de volgende procedures worden onderscheiden:

- Opsporingsonderzoek: de rechter van vrijheid en detentie geeft de machtiging af, op verzoek van de officier van justitie. Indien het plaatsen van het technisch hulpmiddel buiten de wettelijke uren plaatsvindt, moet een aparte machtiging worden afgegeven. De rechter van vrijheid en detentie zal zich in dat geval over beide verzoeken moeten uitspreken.
- Gerechtelijk vooronderzoek: de machtiging wordt in principe afgegeven door de onderzoeksrechter zelf. Als de inzet buiten de wettelijke uren plaatsvindt, dient

[137] In artikel 706-102-5 Sv worden beide routes beschreven.

hiervoor een machtiging van de rechter van vrijheid en detentie te worden verkregen.

Indien wordt gekozen om het technisch hulpmiddel op afstand te plaatsen op het geautomatiseerd werk, wordt de 'normale' route gevolgd zoals beschreven aan het begin van paragraaf 5.6.

5.7 Inzet technische hulpmiddelen vastleggen computergegevens

De Franse wet kent geen specifieke criteria waaraan een technisch hulpmiddel moet voldoen. Informatie over technische hulpmiddelen is staatsgeheim, omdat de middelen ook door de Franse inlichtingendienst kunnen worden gebruikt (persoonlijke communicatie, 29 juni 2022). In Frankrijk is het in beginsel toegestaan om in het strafprocesrecht middelen te gebruiken die staatsgeheim[138] zijn.

Het ontwikkelen van technische hulpmiddelen voor het vastleggen van computergegevens is neergelegd bij het eerdergenoemde STNCJ.[139] De technische hulpmiddelen die kunnen worden gebruikt voor de bevoegdheid zijn dus afhankelijk van het STNCJ. De activiteiten van het STNCJ zijn gekwalificeerd als staatsgeheim, het is dus niet duidelijk welke criteria zij hanteert voor het ontwikkelen of aanschaffen van technische hulpmiddelen.

5.8 Waarborgen

Ten aanzien van het vastleggen van computergegevens geldt een aantal algemene voorwaarden die de kwaliteit van de gegevens moet helpen waarborgen.[140] Allereerst regelt artikel 706-95-18 Sv dat een rapport moet worden opgesteld door de officier van justitie of de onderzoeksrechter (of een door hun aangestelde politieambtenaar), waarin de handelingen en het installeren van het technisch hulpmiddel staan beschreven. Hierin moet onder andere de datum, uur van aanvang en einde van de werkzaamheden worden vermeld. Alleen de gegevens die nodig zijn voor de waarheidsvinding mogen worden gekopieerd. Gegevens die betrekking hebben op het privéleven van de verdachte moeten worden verwijderd. Als de gegevens in een andere taal zijn, moeten deze worden getranscribeerd in het Frans. De gegevens moeten 'verzegeld' bewaard worden, in het geval van de onderhavige bevoegdheid door STNCJ. Bij het verstrijken van de verjaringstermijn worden ze op last van de officier van justitie vernietigd. Van het vernietigen wordt een verslag gemaakt.[141]

5.8.1 Magistratelijke toetsing

De uitvoering van de bevoegdheid vindt plaats onder toezicht van de magistraat die toestemming verleent.[142] In het geval van het opsporingsonderzoek is dit de rechter van vrijheid en detentie en in het geval van het gerechtelijk vooronderzoek de onderzoeksrechter. Deze dient te handelen binnen het gevorderde kader van de

[138] Artikel 3 Besluit van 9 mei 2018 tot oprichting van de dienst met nationale bevoegdheid genaamd 'nationale technische dienst voor gerechtelijke vastlegging'. JORF nr. 0107, 10 mei 2018. (hierna Besluit 9 mei 2018).
[139] Besluit 9 mei 2018.
[140] Deze waarborgen gelden ook voor de inzet van andere bijzondere opsporingsbevoegdheden.
[141] Artikel 706-95-19 Sv.
[142] Artikel 706-95-14 Sv.

officier van justitie. De magistraat kan de inzet van de bevoegdheid op ieder moment afbreken. De officier van justitie moet hiertoe de rechter tijdig informeren over de werkzaamheden die worden uitgevoerd ten behoeve van de bevoegdheid. Als de rechter vaststelt dat de bevoegdheid niet binnen de gestelde kaders is uitgevoerd, moeten de verzamelde gegevens worden verwijderd. Indien de bevoegdheid is ingezet voor andere doeleinden dan opgenomen in het bevel, kunnen de verzamelde gegevens nietig worden verklaard door de zittingsrechter.

5.8.2 Nationale technische dienst voor gerechtelijke vastlegging (STNCJ)

In 2018 is de Nationale technische dienst voor gerechtelijke vastlegging opgericht.[143] Deze organisatie is verantwoordelijk voor het ontwerp, de centralisatie en de implementatie van de technische hulpmiddelen die worden ingezet voor het vastleggen van computergegevens.[144] De dienst coördineert of voert – indien nodig – ook de inzet van de technische hulpmiddelen uit.[145] Zoals reeds opgemerkt zijn de activiteiten van de dienst staatsgeheim.[146] Hierdoor is het onduidelijk welke criteria zij hanteert bij de ontwikkeling of aanschaf van technische hulpmiddelen. Omdat STNCJ verantwoordelijk is voor het verzegelen en bewaren van de gegevens heeft zij een rol bij het beschermen van de integriteit van de verzamelde gegevens.[147]

In 2018 is, op basis van artikel 5 van het Besluit van 9 mei 2018, een strategisch Comité opgericht dat bestaat uit de Minister van Binnenlandse Zaken, de Minister van Justitie en vertegenwoordigers van de diensten die gebruikmaken van de bevoegdheid. Het Comité stelt 'de strategische oriëntaties' en de middelen voor die nodig zijn voor een goede werking van de dienst. Het houdt daarnaast toezicht op de boekhouding en stelt het interne regelement van de dienst vast.[148] Ook schrijft het Comité rapporten over de werkzaamheden van de dienst en een deel daarvan wordt gedeeld met het parlement (persoonlijke communicatie, 12 september 2022). Naast het strategisch comité wijzen de Minister van Binnenlandse Zaken en de Minister van Justitie twee personen aan die toezicht houden op de werkzaamheden van dienst.[149] Deze personen krijgen volledige toegang tot alle technische hulpmiddelen en werkzaamheden van de dienst. Zij kunnen de dienst ook verzoeken aanvullende informatie te verstrekken die zij nodig achten voor het uitoefenen van hun taak. Elk jaar stellen zij een jaarverslag op en deze wordt verstrekt aan de Minister van Binnenlandse Zaken en aan de Minister van Justitie. Dit verslag is niet openbaar en gekwalificeerd als staatsgeheim.

5.8.3 Notificatieplicht en recht op inzage

In de wet is geen notificatieplicht opgenomen. Dit betekent dat een verdachte pas als een zaak ter zitting komt zal worden genotificeerd – mits de inzet van de bevoegdheid bewijsmateriaal oplevert dat is opgenomen in het dossier. 'De verdediging heeft in het gerechtelijk vooronderzoek inzage in de processtukken (artikel 116 Sv) en kan aan de waarheidsvinding een bijdrage leveren door om onderzoekshandelingen te verzoeken (artikel 82-1 SV)' (Verrest, 2018, p. 180).

[143] Besluit 9 mei 2018.
[144] Artikel 2 Besluit 9 mei 2018.
[145] Artikel 2 Besluit 9 mei 2018.
[146] Artikel 3 Besluit 9 mei 2018.
[147] Artikel 706-95-18 Sv.
[148] Artikel 6 Besluit 9 mei 2018.
[149] Artikel 7 Besluit 9 mei 2018.

5.9 Jurisprudentie

In een Joint Investigatory Team (JIT) hebben de Franse en Nederlandse autoriteiten de communicatiedienst EncroChat weten te hacken. Voor korte tijd konden zij alle berichten live meelezen die door criminelen werden uitgewisseld. Omdat de servers in Frankrijk stonden was het de Franse politie die de hack uitvoerde (Goodwin, 2022). De hack heeft in totaal ruim 120 miljoen berichten opgeleverd van 60.000 gebruikers. De berichten zijn in veel landen gebruikt als bewijsmateriaal, verstrekt via een rechtshulpverzoek. Ook in Frankrijk zijn de Encrochatgegevens gegevens gebruikt als bewijsmateriaal. Dit heeft (voorlopig) geleid tot twee arresten die in het kader van onderhavig onderzoek relevant zijn.

Het eerste arrest is van april 2022, hierin oordeelt de Constitutionele Raad (*'le Conseil Constitutionnel'*) dat middelen in het strafprocesrecht kunnen worden ingezet die staatsgeheim zijn.[150] Het gevolg daarvan is dat er geen informatie hoeft te worden gedeeld over de wijze waarop gehackte gegevens zijn verkregen. In oktober 2022 verschijnt echter een arrest van het Hof van Cassatie (*'Cour de cassation'*) waarin het Hof concludeert dat er *wel* aanvullende informatie moet worden gedeeld bij de inzet van de bevoegdheid.[151] Twee van de drie verweren hadden betrekking op de rechtmatigheid van de bevoegdheid en werden verworpen door het Hof, het derde verweer werd deels aangehouden. Op basis van artikel 230-3 Sv moeten, in het geval dat decryptie van gegevens of communicatie plaatsvindt, technische details worden verstrekt over het vastleggen van gegevens. Daarnaast moet een 'certificaat van waarheidsgetrouwheid' worden verstrekt, ondertekend door het hoofd van de uitvoerende technische instantie. In dit certificaat wordt de juistheid en authenticiteit van de gegevens die als bewijsmateriaal worden gebruikt, bevestigd (Goodwin, 2022). Het Hof oordeelt dat er onvoldoende op deze twee criteria is getoetst en verwijst de zaak daarom terug naar de lagere rechter. In een latere uitspraak concludeert het Hof van Cassatie dat het certificaat weliswaar een procedurele verplichting is, maar dat dit alleen nodig is wanneer de verzamelde gegevens versleuteld zijn. In de Encrochatzaak waren de verzamelde gegevens al ontsleuteld voordat ze door de politie werden opgeslagen en was het certificaat dus niet nodig.

5.10 Tot slot

Sinds 2011 is het voor de Franse politie mogelijk om heimelijk op afstand computergegevens vast te leggen op een geautomatiseerd werk. Met het heimelijk vastleggen van computergegevens kunnen in principe alle onderzoekshandelingen worden verricht (afhankelijk van de afgegeven machtiging van de onderzoeksrechter). Een uitzondering is het uitvoeren van surveillance via de aanwezige microfoon of camera op het geautomatiseerd werk. Het is vooralsnog onduidelijk of dit binnen de reikwijdte van de wet valt.

Er gelden enkele algemene waarborgen die ook van toepassing zijn op andere bijzondere opsporingsbevoegdheden. Deze hebben onder meer betrekking op het verzegeld opslaan van verkregen gegevens en de wijze van verslaglegging van uitgevoerde handelingen. Het grootste verschil ten opzichte van Nederland is dat de rechter niet alleen de machtiging afgeeft, maar ook tussentijds toezicht houdt op de uitvoering. Ook mag hij, als daar reden toe is, de inzet op ieder moment afbreken.

[150] Constitutionele Raad, n° 2022-987 QPC, 8 April 2022.
[151] Hof van Cassatie, strafkamer, 11 oktober 2022, beroep nr. 21-85.148.

Daarnaast is een belangrijke waarborg voor de bevoegdheid de aanwezigheid van de dienst STNCJ. Deze dienst geeft, net als Digit in Nederland, uitvoering aan de bevoegdheid en maakt hiervoor gebruik van technische hulpmiddelen. Zij is ook verantwoordelijk voor het bewaren en verzegelen van de gegevens. Anders dan in Nederland kent Frankrijk geen keuringsdienst voor de technische hulpmiddelen. Het STNCJ vervult tot op zekere hoogte ook deze taak. Het is echter niet bekend op welke wijze STNCJ hier invulling aan geeft. Omdat de dienst ook technische hulpmiddelen ontwikkelt voor de inlichtingendienst is het doen en laten van de dienst minder publiekelijk dan Digit. Ditzelfde geldt voor het toezicht op STNCJ. Publicaties van de toezichthouders over het doen en laten van de dienst zijn niet openbaar (staatsgeheim). Dit staat in contrast met de werkzaamheden van de Inspectie in Nederland, waarvan wel een openbaar rapport verschijnt. Opvallend is STNCJ zowel 'keurder' als 'uitvoerder' is. Dit roept de vraag op in hoeverre STNCJ onafhankelijk beide rollen kan vervullen. Het feit dat de dienst de inzet uitvoert wordt echter gezien als een waarborg *an sich* door de wetgever en de bevindingen van STNCJ worden als betrouwbaar gezien in de rechtbank.

6 Zweden

Met speciale dank aan Johanna Rådberg (politie, Zweden), Chatrine Rudström (Openbaar Ministerie, Zweden), Pär Runemar (politie, Zweden) en Staffan Uhlmann (ministerie van Justitie, Zweden) voor het kritische meelezen van dit hoofdstuk op feitelijke onjuistheden.

6.1 Wettelijke regeling

Op 1 april 2020 is in Zweden de wet 'Heimelijke gegevensuitlezing' (Whg) ('*Lag om hemlig dataavläsning*') in werking getreden.[152] Op basis van deze wet is het voor de Zweedse politie mogelijk om heimelijk op afstand informatie van een geautomatiseerd werk[153] te lezen of op te nemen.[154] Indien nodig mag daarvoor de beveiliging van een geautomatiseerd werk worden doorbroken.[155] De introductie van de wet werd om twee redenen noodzakelijk geacht door de wetgever: (1) de behoefte om in het geheim toegang te krijgen tot informatie die door technologische en maatschappelijke ontwikkelingen met bestaande dwangmaatregelen (vergelijkbaar met de bestaande opsporingsbevoegdheden) niet meer toegankelijk zijn; en (2) de behoefte om in het geheim gegevens te verzamelen over de werking en het gebruik van geautomatiseerde werken die via bestaande dwangmaatregelen niet kunnen worden verzameld.[156]

Op basis van de bevoegdheid kunnen verschillende type gegevens worden vastgelegd:[157]

1 Interceptiegegevens: gegevens over de inhoud van berichten die van of naar een telefoonnummer of (IP-)adres worden verzonden.
2 Communicatiegegevens: niet inhoudelijke (meta-)gegevens over de communicatie die van of naar een telefoonnummer of (IP-)adres plaatsvindt.
3 Locatiegegevens: informatie over de locatie van het geautomatiseerd werk.
4 Camerагegevens: informatie verkregen via de camera van het geautomatiseerd werk.
5 Fysieke interceptiegegevens: gegevens verzameld met behulp van de microfoon van het geautomatiseerd werk in fysieke ruimtes.
6 Gegevens die zijn opgeslagen op het geautomatiseerd werk.
7 Gegevens over het gebruik van het geautomatiseerd werk.

Anders dan de naam van de wet mogelijk doet vermoeden, kunnen op basis van de wet niet alleen opgeslagen maar ook stromende gegevens worden verzameld. Hierbij mogen de aanwezige camera en microfoon worden aangezet om gegevens te verkrijgen.

[152] *Lag (2020:62) om hemlig dataavläsning Svensk författningssamling*.
[153] In Zweden wordt gesproken over een 'leesbaar informatiesysteem' ('*avläsningsbart informationssystem-informationssystem*'), wat gedefinieerd wordt als: 'een elektronisch communicatieapparaat of gebruikers-account, of een gelijkwaardig afgebakend deel, voor een communicatiedienst, opslagdienst of soortgelijke dienst' (sectie 1 Whg).
[154] Sectie 1 Whg.
[155] Sectie 22 Whg.
[156] Wetsvoorstel Whg, p. 68-73.
[157] Sectie 2 Whg.

6.2 Bevoegde autoriteiten

In Zweden kunnen zowel de politie als de officier van justitie een vooronderzoek (opsporingsonderzoek) starten. De persoon die leidinggeeft aan het vooronderzoek wordt aangeduid als de 'hoofdonderzoeker' ('*undersökningsledaren*') (Wong, 2012, p. 3-4). De officier van justitie neemt de leiding van een onderzoek over op het moment dat een verdachte in beeld is.[158] De hoofdonderzoeker bepaalt welke opsporingsbevoegdheden gedurende een onderzoek worden ingezet en hoe en wanneer het onderzoek is afgerond. De daadwerkelijke onderzoekshandelingen – zoals het verhoor en het uitvoeren van de opsporingsbevoegdheden – worden in de praktijk uitgevoerd door de politie. Voor een deel van deze handelingen – zoals surveillance-bevoegdheden – is een bevel van de rechter nodig (Wong, 2012, p. 4).

Omdat de bevoegdheid heimelijke gegevensuitlezing in beginsel alleen kan worden uitgevoerd als een verdachte in beeld is, is het in de praktijk de officier van justitie die het bevel geeft de heimelijke gegevensuitlezing in een opsporingsonderzoek in te zetten.[159] Voor de inzet van de bevoegdheid is op basis van sectie 15 Whg een rechterlijke machtiging nodig. Naast de rechter is een zogenaamde publieke vertegenwoordiger betrokken die het belang van de verdachte behartigt bij de beoordeling van de aanvraag.[160] In geval van spoed kan de officier van justitie zelf toestemming verlenen in afwachting van het oordeel van de rechter.[161] De officier van justitie dient de rechter 'zonder vertraging' te informeren.

In de wet wordt niet beschreven welk onderdeel van de politie belast is met het daadwerkelijk uitvoeren van de bevoegdheid. In een interview met de Zweedse politie komt naar voren dat dit in de praktijk is belegd bij een technisch onderlegd team van de politie (persoonlijke communicatie, 6 juli 2022).

6.3 Tegen wie

Analoog aan de bestaande interceptiebevoegdheden in Zweden, mag de bevoegdheid in beginsel alleen worden ingezet tegen iemand ten aanzien van wie een sterke verdenking bestaat.[162] Op basis van sectie 4 Whg mag de bevoegdheid verder alleen worden ingezet op het geautomatiseerd werk dat in gebruik is bij de verdachte. Wel biedt sectie 4 Whg de mogelijkheid om in het kader van interceptie van communicatie de bevoegdheid in te zetten op een geautomatiseerd werk waarbij een sterk vermoeden bestaat dat de verdachte hiermee contact zal hebben (bijvoorbeeld een telefoon van een geliefde). Sectie 5 Whg biedt daarnaast een tweede uitzondering, namelijk in situaties waarin een geautomatiseerd werk wordt aangetroffen dat gebruikt is gedurende het misdrijf of samenhangt met het plaats delict. In dat geval kan de bevoegdheid worden ingezet voor het achterhalen van de communicatie- en locatiegegevens om achter de mogelijke identiteit van een verdachte te komen.

[158] Hoofdstuk 23, artikel 3 Sv. Indien gewenst kan de officier van justitie op basis van dit artikel ook in andere gevallen met 'speciale redenen onderbouwd' het onderzoek overnemen.
[159] Sectie 5 Whg biedt een uitzondering namelijk dat de bevoegdheid kan worden ingezet om de identiteit van een verdachte te achterhalen. In dit geval kan het zijn dat de politie nog de leiding heeft over het onderzoek. Wel moet het technisch hulpmiddel altijd worden ingezet door de officier van justitie in overeenstemming met sectie 14 Whg.
[160] Sectie 16 Whg. Zie ook paragraaf 6.6.1.
[161] Sectie 17 Whg.
[162] Wetsvoorstel Whg, p. 109. Hoofdstuk 27, artikel 20 Sv.

6.4 Gevallen

Bij het vooronderzoek mag de bevoegdheid worden ingezet voor misdrijven waarvoor minimaal een gevangenisstraf van twee jaar kan worden opgelegd.[163] Daarnaast wordt in sectie 4 Whg een aantal specifieke misdrijven genoemd waarvoor de bevoegdheid mag worden ingezet. Het gaat onder meer om: sabotage, brandstichting, bedreigingen tegen de rechtsorde, (bedrijfs-)spionage door buitenlandse mogendheden en terrorisme.[164] Dit geldt ook voor een poging tot, voorbereiding van of het aanzetten tot de hierboven genoemde misdrijven.[165]

Buiten het vooronderzoek mag de bevoegdheid voor een aantal andere specifieke doeleinden worden ingezet. Allereerst mag de bevoegdheid worden ingezet ter preventie van 'bijzonder zware' misdrijven ('*särskilt allvarliga brott*').[166] Het gaat hier om bovenstaande misdrijven aangevuld met moord, doodslag, zware mishandeling, ontvoering of onrechtmatige vrijheidsbeneming.[167] De bevoegdheid mag ook worden ingezet als sprake is van een 'tastbaar' risico dat een persoon of een groep één van deze misdrijven zal plegen. Daarnaast mag de politie heimelijk gegevens verzamelen ter uitvoering van de Vreemdelingenwet, bijvoorbeeld bij een besluit tot uitzetting.[168] Omdat het hier gaat om specifieke uitzonderingen en/of preventieve maatregelen ligt de focus in de rest van het hoofdstuk op het gebruik van heimelijke gegevensuitlezing in het vooronderzoek.

In sectie 11 Whg is een aantal situaties geregeld waarin de bevoegdheid niet mag worden ingezet. Heimelijke gegevensuitlezing is niet toegestaan als de inzet op een geautomatiseerd werk de persvrijheid beperkt en als een geheimhouder zoals een advocaat, arts of priester het geautomatiseerd werk gebruikt.

6.5 Termijn

De bevoegdheid mag niet langer dan noodzakelijk worden ingezet. Er geldt een maximale termijn van één maand. Deze termijn kan telkens met één maand worden verlengd. Voor historisch opgeslagen data, zoals tekstberichten op een telefoon, geldt geen termijn. Dit betekent dat historische tekstberichten of mailtjes kunnen worden gelezen en opgeslagen die buiten de termijn opgenomen in de machtiging zijn verstuurd.[169] Overigens kan de rechter besluiten dat alleen gegevens binnen een bepaalde periode mogen worden bevraagd.

6.6 Formaliteiten

Voor de inzet van de bevoegdheid in een vooronderzoek dient de officier van justitie een rechterlijke machtiging aan te vragen.[170] Een bevel kan alleen worden afgegeven voor misdrijven genoemd in paragraaf 6.4 en mag op basis van sectie 3 Whg alleen worden verleend als de redenen voor de inzet van de bevoegdheid zwaarder wegen

[163] Sectie 4 Whg.
[164] Hoofdstuk 27, artikel 18, lid 2 tot en met 7 Sv.
[165] Hoofdstuk 27, artikel 18, lid 8 Sv.
[166] Sectie 7 Whg.
[167] Sectie 1, Wet (2007:979) betreffende maatregelen ter voorkoming van bepaalde bijzonder ernstige misdrijven ('*Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott*').
[168] Sectie 9 Whg.
[169] SIN Besluit, 2021, p. 6.
[170] Sectie 15 Whg.

dan de inbreuk die de bevoegdheid maakt (proportionaliteitstoets). In de interviews komt naar voren dat de beoordeling van de rechter zich concentreert op de bepalingen in de Whg en aanverwante bepalingen. Het is onduidelijk in hoeverre de rechter kijkt naar de techniek van de hulpmiddelen en naar de waarborgen die hiermee samenhangen. Uit een besluit van de Zweedse Commissie voor Veiligheid en Integriteitsbescherming (*'Säkerhets- och integritetsskyddsnämnden'*, hierna SIN) komt naar voren dat technisch experts van de politie soms gehoord worden door de rechter.[171] Op basis van dit besluit en informatie uit interviews blijkt dat de focus ligt op de technische aspecten die van invloed zijn op de proportionaliteit van de inzet, bijvoorbeeld de onderzoekshandelingen die kunnen worden verricht met het middel.

In de machtiging moet op basis van sectie 18 Whg een aantal onderdelen worden opgenomen. Allereerst de startdatum en de termijn waarvoor een machtiging wordt afgegeven. Ten tweede moet worden vastgelegd op welk geautomatiseerd werk het bevel betrekking heeft (zie paragraaf 6.3). Ten derde moet worden aangegeven welk type gegevens mag worden gelezen of vastgelegd, denk bijvoorbeeld aan communicatiegegevens en cameragegevens (zie paragraaf 6.1). Ten vierde moet worden vastgelegd welke maatregelen worden genomen om de inbreuk op de verdachte of betrokkene te minimaliseren. Een voorbeeld hiervan is dat de camera of microfoon op een geautomatiseerd werk alleen op een bepaalde locatie of tijd mag worden geactiveerd.

6.6.1 Publieke vertegenwoordiger

Zodra de rechtbank van de officier van justitie een aanvraag ontvangt om de bevoegdheid te mogen inzetten, moet de rechtbank zo snel mogelijk een publieke vertegenwoordiger aanwijzen.[172] Deze publieke vertegenwoordiger moet een Zweeds staatsburger zijn en een advocaat of gewone rechter zijn (geweest).[173] Publieke vertegenwoordigers dienen de privacybelangen van de verdachte te beschermen bij de beoordeling van de aanvraag. De vertegenwoordiger heeft het recht om deel te nemen aan de bijeenkomst waarin besproken wordt wat er in de zaak naar voren komt en hij/zij mag adviseren over de aanvraag. Het advies van de vertegenwoordiger is niet bindend voor de beoordeling van de rechter. Wel kan de vertegenwoordiger, indien hij of zij het niet eens is met het oordeel van de rechter, in beroep gaan tegen zijn/haar beslissing.[174]

6.7 Technische hulpmiddelen

Na afgifte van de machtiging kan de politie ieder technisch hulpmiddel (doorgaans software) gebruiken dat benodigd is om gegevens te lezen en op te slaan.[175] De enige beperking die in de wet staat opgenomen, is dat het technisch hulpmiddel moet zijn aangepast aan de toestemming in het bevel.[176] In sectie 23 Whg staat genoemd dat het technisch hulpmiddel zodanig moet zijn aangepast dat het niet mogelijk is om informatie te lezen of op te slaan anders dan gespecificeerd in het bevel. Het technisch hulpmiddel hoeft niet specifiek voor één doeleinde te zijn ontwikkeld. Zolang de politie kan aantonen dat de software is ingezet om *alleen* de gegevens te lezen en vast te

[171] SIN besluit, nr. 92-2020.
[172] Sectie 16 Whg.
[173] Hoofdstuk 27, artikel 27 Sv.
[174] Hoofdstuk 27, artikel 26 Sv.
[175] Sectie 22 Whg.
[176] Sectie 23 Whg.

leggen uit het bevel, is dat voldoende om te voldoen aan de voorwaarde in sectie 23 Whg. Indien toch blijkt dat gegevens zijn vastgelegd die buiten het bevel vallen, dienen deze direct te worden verwijderd en dient een melding te worden gemaakt bij SIN. In paragraaf 6.8.2 wordt nader ingegaan op de rol van deze commissie.

6.8 Waarborgen

In de wet worden weinig formele waarborgen genoemd ten aanzien van de kwaliteit van de gegevens verkregen met heimelijke gegevensuitlezing. Wel worden in sectie 25 en 26 Whg een aantal zorgvuldigheidsvereisten genoemd. Verder kent Zweden SIN die toezicht houdt op de wijze waarop onder meer de heimelijke gegevenslezing wordt uitgevoerd. Daarnaast hanteert de politie een aantal interne richtlijnen hoe om te gaan met de bevoegdheid. Deze richtlijnen zijn niet openbaar. Ten slotte geldt een notificatieplicht en krijgt de verdachte een kopie van de met de bevoegdheid verkregen gegevens. In de komende subparagrafen worden de zojuist genoemde punten nader besproken.

6.8.1 Zorgvuldigheidsvereisten

In secties 25 en 26 Whg worden zorgvuldigheidsvereisten genoemd die indirect van invloed kunnen zijn op de kwaliteit van de verzamelde gegevens afkomstig van het geautomatiseerd werk. De eisen zijn er primair op gericht dat de verrichte handelingen niet meer overlast of schade veroorzaken aan het geautomatiseerd werk van de verdachte dan strikt noodzakelijk voor de uitvoering van de bevoegdheid. Na het beëindigen van de inzet dient het technisch hulpmiddel te worden verwijderd en de beveiliging van het geautomatiseerd werk op zijn minst op hetzelfde niveau te zijn als vóór de inzet. Daarnaast wordt in sectie 26 Whg genoemd dat de personen die de bevoegdheid uitvoeren over voldoende kennis en kwalificaties dienen te beschikken om de bevoegdheid uit te voeren.

6.8.2 Commissie voor Veiligheid en Integriteitsbescherming (SIN)

SIN houdt toezicht op het gebruik van bijzondere opsporingsbevoegdheden door de politie en de geheime dienst.[177] Als gevolg daarvan houdt SIN ook toezicht op de wijze waarop de politie de heimelijke gegevensuitlezing inzet. Het doel van SIN is om (1) te controleren of bijzondere opsporingsbevoegdheden conform wet- en regelgeving zijn ingezet; en (2) of persoonsgegevens conform wet- en regelgeving zijn verwerkt.[178] De commissie bestaat uit maximaal tien personen. De voorzitter en vicevoorzitter hebben een juridische achtergrond (bijvoorbeeld een rechter) en de rest van de commissie bestaat uit leden van politieke partijen in het parlement (persoonlijke communicatie, 12 september 2022). De commissie heeft beperkte technische kennis in huis, en kan indien nodig aanvullend een deskundig persoon aanstellen om de commissie bij te staan.[179]

Op het moment dat een rechterlijke machtiging voor heimelijke gegevenslezing wordt afgegeven, is de rechtbank verplicht SIN te notificeren.[180] SIN kan in theorie iedere

[177] Wet (2007:980) op toezicht over bepaalde politie-activiteiten(‘*Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet*’).
[178] Sectie 3, Wet (2007:980) op toezicht over bepaalde politie-activiteiten.
[179] Artikel 18, Verordening (2007:1141) met instructie voor de Commissie voor Veiligheid en Integriteitsbescherming (‘*Förordning (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden’*).
[180] Sectie 21 Whg.

willekeurige zaak waarvan zij op de hoogte wordt gesteld aan haar toezicht onderwerpen. In reactie op schriftelijke vragen geeft SIN aan dat de selectie van zaken waarnaar zij kijkt steekproefsgewijs plaatsvindt. Daarnaast kan de selectie plaatsvinden op basis van onregelmatigheden in de notificatie, bijvoorbeeld omdat het misdrijf in beginsel niet in aanmerking komt voor de inzet van de bevoegdheid (persoonlijke communicatie, 26 augustus 2022). Ook is SIN verplicht om op verzoek van individuen, bijvoorbeeld een verdachte tegen wie de bevoegdheid is ingezet, te controleren of de bevoegdheid tegen hen in overeenstemming met de wet is ingezet.[181] SIN moet de persoon op de hoogte stellen van de door haar uitgevoerde controle. Indien het verzoek van het individu 'onredelijk' of 'ongegrond' is in de ogen van SIN, dan hoeft geen controle plaats te vinden.

Als SIN onregelmatigheden vaststelt, doet zij een uitspraak. De uitspraken van SIN zijn niet bindend, maar in een schriftelijke reactie geeft SIN aan dat de organisaties zich in beginsel conformeren aan de uitspraken van SIN en hun interne richtlijnen daarop aanpassen (persoonlijke communicatie, 29 september 2022). Indien onregelmatigheden dermate ernstig zijn dat het strafbaar is (bijvoorbeeld als sprake is van ambtsmisbruik) dan wordt dit gemeld bij het Openbaar Ministerie die eventueel over kan gaan tot vervolging (persoonlijke communicatie, 26 augustus 2022; Cameron, 2021, p. 1365).

In wet- en regelgeving zijn – naast de rechtmatigheidstoets – geen aanvullende criteria opgenomen waarop het toezicht van SIN zich richt. SIN maakt geen gebruik van een inspectieprotocol. In de schriftelijke reactie van SIN geeft zij aan dat het toezicht op de heimelijke gegevensuitlezing nog in ontwikkeling is (persoonlijke communicatie, 26 augustus 2022). Wel zijn in 2021 twee uitspraken verschenen die iets meer duidelijkheid verschaffen over de criteria waarnaar wordt gekeken:[182]

- het voldoen aan grondwettelijke voorwaarden;
- de periode van heimelijke gegevenslezing;
- de proportionaliteit van de inzet in relatie tot het type gegevens dat wordt bevraagd tijdens de inzet;
- de aanwezigheid van voorwaarden in het bevel om de persoonlijke integriteit van de verdachte te waarborgen;
- het uitvoeren van de bevoegdheid in relatie tot overige voorwaarden in het bevel;
- vereisten van zorgvuldigheid en nauwkeurigheid bij de inzet van de bevoegdheid.

Hoewel de beschreven voorwaarden vooral juridisch of procesmatig van aard zijn, kunnen deze criteria ook betrekking hebben op de gebruikte technische hulpmiddelen, bijvoorbeeld de functionaliteiten waarover een technisch hulpmiddel beschikt. Als een technisch hulpmiddel onbedoeld meer informatie verstrekt dan in het bevel is opgenomen, is de officier van justitie verplicht dit te melden bij SIN. Daarnaast kan SIN dit zelf vaststellen tijdens diens toezicht, wat er toe kan leiden dat een technisch hulpmiddel niet langer kan worden gebruikt of aangepast dient te worden (persoonlijke communicatie, 29 september 2022).

6.8.3 Interne richtlijnen heimelijke gegevensuitlezing

Hoewel in de wet weinig formele waarborgen zijn opgenomen ten aanzien van de kwaliteit van de verkregen gegevens met heimelijke gegevensuitlezing, hanteert de

[181] Sectie 3, Wet (2007:980) op toezicht over bepaalde politie activiteiten.
[182] Nummer 96-2022 Statement SIN, Number 92-2020 Statement SIN.

politie een aantal interne richtlijnen over de omgang met de bevoegdheid en de inzet van technische hulpmiddelen. Deze richtlijnen zijn op dit moment in ontwikkeling.[183]

De interne richtlijnen van de politie zijn vertrouwelijk en niet openbaar beschikbaar. Hierdoor hebben wij niet kunnen vaststellen welke interne criteria de politie precies hanteert ten aanzien van de kwaliteit van de gegevens verkregen met de bevoegdheid tot heimelijke gegevensuitlezing. Uit interviews komt naar voren dat de politie gebruikmaakt van gestandaardiseerde of gecertificeerde software (persoonlijke communicatie, 13 december 2022). Aangegeven wordt dat ten tijde van de zitting dit gebruikt kan worden als één van de argumenten waarmee wordt aangetoond dat de integriteit van de gegevens verwerkt met deze software gewaarborgd is. Voor software die niet specifiek voor heimelijke gegevensuitlezing wordt gebruikt, kan het Zweeds nationaal forensische instituut de technische hulpmiddelen evalueren. Dit gaat bijvoorbeeld om technische hulpmiddelen waarmee uitgelezen gegevens (verder) kunnen worden geanalyseerd. Deze middelen worden niet ingezet om een geautomatiseerd werk binnen te dringen, maar kunnen in een latere fase van de heimelijke gegevensuitlezing – nadat de gegevens zijn verkregen – worden ingezet. Daarnaast wordt aangegeven dat gebruik wordt gemaakt van technische hulpmiddelen die gelden als de standaard binnen andere politiediensten[184] of door hen zijn gecertificeerd (bijvoorbeeld door de Nederlandse Keuringsdienst).

6.8.4 Notificatieplicht en recht op inzage

Op basis van sectie 28 Whg jo. Art. 31 hoofdstuk 27 Sv geldt een notificatieplicht aan betrokkenen. In beginsel dient op basis van artikel 31, hoofdstuk 27 Sv een persoon zo spoedig mogelijk te worden genotificeerd en uiterlijk één maand nadat het voor-onderzoek is afgerond. In de notificatie dient te worden opgenomen welke bijzondere opsporingsmiddelen zijn ingezet en wanneer de inzet daarvan heeft plaatsgevonden. Daarbij moet worden vermeld op welke telefoonnummers, (IP-) adressen en geauto-matiseerde werken de inzet betrekking had. Indien sprake was van fysieke interceptie van beeld of geluid dient informatie te worden opgenomen over de plekken waar deze interceptie heeft plaatsgevonden.[185] Op basis van artikel 33, hoofdstuk 27 Sv kan een melding achterwege blijven als het vooronderzoek betrekking heeft op de in lid 1 tot en met 7 beschreven misdrijven. Dit zijn voornamelijk misdrijven die een gevaar vormen voor de bevolking of nationale veiligheid. Veel van de misdrijven waarvoor heimelijke gegevensuitlezing kan worden ingezet vallen hier onder.

Indien de officier van justitie besluit om over te gaan tot vervolging en de zaak ter zitting komt, zal dit in veel gevallen het moment zijn dat een verdachte wordt genotificeerd. De verdachte krijgt inzage in het bewijsmateriaal dat in de rechtszaak wordt gebruikt. De verdachte kan, onderbouwd, vragen om aanvullende gegevens die zijn verzameld. In het geval van heimelijke gegevensuitlezing betekent dit dat de verdachte een kopie krijgt van alle verzamelde gegevens. In interviews met Zweedse respondenten komt naar voren dat experts als getuige kunnen worden opgeroepen, indien er vragen zijn over de kwaliteit van de gegevens. De officier van justitie kan de betrokken politieambtenaar als getuige oproepen om toe te lichten welke handelingen

[183] Number 92-2020 Statement SIN. Zie ook de uitspraak van SIN naar aanleiding van een zaak waarin de bevoegdheid op een verkeerde telefoon is ingezet. Dit heeft geleid tot aanpassing van de interne richtlijnen van de politie om meer controles in het proces op te nemen om te voorkomen dat het technisch hulpmiddel op het verkeerde geautomatiseerd werk wordt ingezet (Nummer 96-2022 Statement SIN).

[184] Een voorbeeld van dit type software is Cellebrite dat door veel politiediensten wordt gebruikt om telefoons uit te lezen.

[185] Sectie 29 Whg jo. art. 32, hoofdstuk 27 Sv.

zijn verricht en waarom de kwaliteit van de gegevens is gewaarborgd (persoonlijke communicatie, 13 december 2022). Er wordt echter geen informatie gedeeld over de gebruikte technische hulpmiddelen of modus operandi van de politie (persoonlijke communicatie, 13 december 2022). Verder kent Zweden op basis van artikel 1, hoofdstuk 35 Sv een flexibele ontvankelijk en vrije evaluatie van bewijs. Dit wil zeggen dat in beginsel al het bewijs ontvankelijk is, ongeacht hoe het verkregen is. Het is aan de rechter om te wegen hoe relevant het bewijs is (Klamberg, 2020). De wijze waarop het bewijs is verkregen, kan van invloed zijn op de beoordeling. Als het bewijs overduidelijk onrechtmatig is verkregen kan de rechter besluiten het bewijs uit te sluiten.

6.9 Jurisprudentie

In een brief aan het parlement komt naar voren dat sinds de invoering van de wet de bevoegdheid in 205 opsporingsonderzoeken is ingezet.[186] Voor zover bekend is er nog geen jurisprudentie beschikbaar van zaken waarin de bevoegdheid is ingezet. Wel zijn er een paar uitspraken in zaken die betrekking hebben op bewijsmateriaal verkregen uit Encrochat-communicatie. In deze zaken is ook de kwaliteit van de verkregen gegevens ter discussie gesteld. Daarnaast is een uitspraak van SIN verschenen naar aanleiding van een onjuiste inzet van de bevoegdheid.

Op 26 februari en 22 april 2021 heeft het Hof van beroep twee uitspraken gedaan in zaken waarin Encrochat-communicatie[187] als bewijsmateriaal werd aangevoerd.[188] In beide zaken voerde de verdediging vergelijkbare argumenten aan. Het eerste bezwaar had betrekking op de rechtmatigheid van het bewijs en dit werd afgewezen door de rechter. Omdat dit geen betrekking heeft op de kwaliteit van de verkregen gegevens wordt daar op deze plek niet verder op ingegaan. Ten aanzien van de kwaliteit van de gegevens zijn verschillende punten ter discussie gesteld. Zo ontbreken er berichten, hebben sommige berichten dezelfde afzendertijd waardoor ze mogelijk in de verkeerde volgorde worden gelezen en zijn de gegevens verschillende keren bewerkt (gekopieerd door de politie). De rechtbank erkent dat de gegevens onvolledig zijn en dat het van belang is de berichten zorgvuldig in hun context te beoordelen. De rechtbank vervolgt dat de gegevens in samenhang met andere opsporingsgegevens laten zien dat 'de berichten qua tijd en inhoud goed overeenkomen met de werkelijkheid'.[189] In beide zaken heeft de rechtbank de bezwaren van de verdediging verworpen.

Naast deze twee uitspraken verscheen op 16 november 2021 een uitspraak van SIN naar aanleiding van een onjuiste inzet van de heimelijke gegevensverzameling in een opsporingsonderzoek. In het betreffende onderzoek was de bevoegdheid per abuis ingezet op een mobiele telefoon die niet onder het bevel viel. Bij het ontdekken van de fout is de inzet van de bevoegdheid stopgezet en zijn de gegevens direct verwijderd. SIN concludeert in haar uitspraak dat hiermee niet aan de vereisten van zorgvuldigheid en nauwkeurigheid is voldaan en dat eerder passende maatregelen hadden moeten worden getroffen.[190] Naar aanleiding van de uitspraak heeft de politie haar

[186] Regeringsbrief 2022/23.30, Verantwoording gebruik heimelijke dwangmiddelen in 2021. In 2021 ging het om 145 opsporingsonderzoeken en in 2020 (vanaf april) ging het om 60 opsporingsonderzoeken.
[187] Zie paragraaf 5.9.
[188] Uitspraak Hof van beroep nr. B 210-21 & nr. B 5546-20.
[189] Uitspraak rechtbank Stockholm d.d. 22 april 2021 in zaak nr. B 5546-20, p. 9.
[190] Nummer 96-2022 Statement SIN, p. 1.

werkwijze aangepast. Zij voert meerdere controles uit om zeker te zijn dat de bevoegdheid op het juiste systeem wordt ingezet.[191]

6.10 Tot slot

Op basis van de wet heimelijke gegevensuitlezing is het voor de Zweedse politie mogelijk om heimelijk op afstand de beveiliging van een geautomatiseerd werk te doorbreken en de gegevens te lezen die daarop staan opgeslagen. Op basis van de wet kunnen de volgende type gegevens worden uitgelezen: interceptiegegevens, communicatiegegevens, locatiegegevens, camerагegevens, fysieke interceptie-gegevens, gegevens op het geautomatiseerd werk en gegevens over het gebruik van het geautomatiseerd werk. De wet stelt geen specifieke eisen aan de technische hulpmiddelen die kunnen worden gebruikt (commercieel of zelf ontwikkeld).

Ten aanzien van de kwaliteit van de gegevens verkregen met de bevoegdheid zijn vrijwel geen formele wettelijke vereisten opgenomen in de wet. Wel zijn er interne beleidsregels bij de politie waarin nadere processen en eisen rondom het gebruik van technische hulpmiddelen zijn opgenomen. Deze richtlijnen zijn helaas niet openbaar waardoor onduidelijk is wat deze inhouden. Opvallend – in vergelijking met Nederland – is dat de belangrijkste controle ten aanzien van de inzet van de technische hulpmiddelen *ex post* plaatsvindt door toezichthouder SIN. SIN houdt toezicht op de inzet van bijzondere opsporingsbevoegdheden, waaronder heimelijke gegevensuitlezing. De rol van SIN ten aanzien van de inzet van de technische hulp-middelen voor heimelijke gegevensuitlezing is nog in ontwikkeling. Het toezicht richt zich vooralsnog primair op juridische en procesmatige aspecten van de bevoegdheid, vergelijkbaar met die van de Inspectie in Nederland. Anders dan in Nederland kan SIN ook de rechtmatigheid van het hele proces toetsen, van zowel de politie als van het Openbaar Ministerie. SIN kan daarnaast publiekelijk uitspraken doen in individuele zaken. De verdachte kan hier persoonlijk om vragen.

[191] Nummer 96-2022 Statement SIN, p. 3.

7 Zwitserland

Dit hoofdstuk is gecontroleerd op feitelijke onjuistheden door een jurist uit Zwitserland. Deze persoon vond het niet nodig bij naam te worden genoemd.

7.1 Wettelijke regeling

Sinds 1 maart 2018 kent het Zwitserse Wetboek van Strafvordering (‘*Schweizerisch Strafprozessordnung*’) artikel 269ter waarin de hackbevoegdheid is geregeld. Dit artikel is aangekondigd in de toelichting (‘*Botschaft*’) behorende bij de revisie van de BÜPF, de Federale wet surveillance van post- en telecommunicatie (‘*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs*’).[192] Een belangrijke aanleiding voor dit nieuwe wetsartikel was de versleuteling van communicatie-(gegevens) waardoor reeds bestaande bevoegdheden voor de politie geen bruikbare informatie meer opleverden.[193] In lid 1 van artikel 269ter Sv is geregeld dat de officier van justitie een bevel mag geven om speciale software (‘*besonderen Informatik-programmen*’) te installeren in een geautomatiseerd werk (‘*Datenverarbeitungs-system*’) dat voor gegevensverwerking wordt gebruikt. De speciale software wordt aangeduid als Government Software, ook wel GovWare (zie oa EJPD, 2019). Met behulp van GovWare mogen alleen communicatie en de metadata van telecommunicatie worden onderschept.

Vóór de introductie van de zojuist beschreven bevoegdheid werd gediscussieerd over de vraag of reeds bestaande wetsartikelen niet al voldoende wettelijke basis boden om GovWare te installeren, bijvoorbeeld situaties waarin het parket (‘*Staatsanwaltschaft*’) technische monitorapparatuur (‘*Überwachungsgeräte*’) mag gebruiken.[194] Een meerderheid van de wetenschappers was echter van mening dat dit op basis van dat artikel niet toegestaan was, terwijl sommigen meenden dat dit wel mogelijk zou kunnen zijn, mits artikel 280 Sv op een brede manier geïnterpreteerd werd.[195] Ten tijde van de introductie van het nieuwe wetsartikel had het Federale Hooggerechtshof (‘*das Bundesgericht*’) hier nog niet over geoordeeld[196] en op het moment van schrijven van dit rapport is dat nog steeds het geval (zie later). Verder is bekend dat vóór de introductie van het nieuwe Zwitserse Wetboek van Strafvordering in 2011 justitiële autoriteiten GovWare hebben ingezet. Dat gebeurde destijds op basis van bestaande federale wetten en wetten in de kantons[197] (Basanisi, 2019, p. 2). Zwitserland is opgedeeld in 26 verschillende deelstaten (kantons). Daarnaast kent Zwitserland een centrale staat (ProDemos, 2022).

[192] Sinds de komst van het gemoderniseerde Wetboek van Strafvordering in 2011 zijn de strafvorderlijke wetten uit de BÜPF overgeheveld naar het nieuwe Wetboek van Strafvordering. Om die reden worden in de revisie van de BÜPF ook wijzigingen geïntroduceerd in het Wetboek van Strafvordering (Botschaft 27 februari 2013, p. 2690). De introductie van artikel 269ter Sv is er daar één van. Opname in het Wetboek van Strafvordering stemt verder overeen met een aantal moties dat is ingediend (Botschaft 27 februari 2013, p. 2777).
[193] Botschaft 27 februari 2013, p. 2775.
[194] Hansjakob (2011, p. 5) beargumenteert waarom dit artikel niet gebruikt zou kunnen worden. Ook het oude artikel 269 Sv zou geen wettelijke grondslag bieden voor het gebruik van GovWare (Hansjakob, 2011, p. 4).
[195] Botschaft 27 februari 2013, p. 2772.
[196] Botschaft 27 februari 2013, p. 2772.
[197] Botschaft 27 februari 2013, p. 2772-2773.

Zoals eerder beschreven is artikel 269ter Sv gericht op het onderscheppen van (versleutelde) communicatie. Op basis van dit artikel is het niet toegestaan een online doorzoeking[198] te doen of om een camera of microfoon van een computer voor andere doeleinden te gebruiken dan het monitoren van telecommunicatie. Ook is het observeren van een ruimte met behulp van Govware niet toegestaan.[199] Indien andere gegevens dan communicatiegegevens worden verzameld, mogen deze niet worden gebruikt als bewijs en moeten deze worden vernietigd.[200]

7.2 Bevoegde autoriteiten

Zoals eerder genoemd is Zwitserland opgedeeld in 26 kantons en een centrale staat. Een dergelijke tweedeling is ook terug te zien binnen de verschillende instituties die opereren binnen het strafproces. In principe worden veel strafzaken afgehandeld op het niveau van de kantons. Voor enkele strafzaken gebeurt dat op federaal niveau. Daarbij gaat het om onderzoeken naar georganiseerde criminaliteit, delicten tegen de Staat en economische delicten, waaronder witwassen. Een belangrijke voorwaarde hierbij is dat de delicten grotendeels in het buitenland zijn gepleegd of dat het om een zaak gaat die meerdere kantons betreft en er 'geen duidelijk zwaartepunt van de strafbare feiten te bepalen valt'. Indien van het voorgaande sprake is, kunnen kantons zaken bij een federale rechter laten behandelen. In dat geval zal het federaal Openbaar Ministerie een onderzoek instellen[201] (Godenzi & Caprara, 2018, p. 284).
Het gebruik van GovWare is, zoals eerder genoemd, alleen toegestaan als een officier van justitie (op federaal niveau of op het niveau van de kantons) hiervoor een bevel afgeeft.[202]

Naast een bevel van de officier van justitie is autorisatie door een rechter van de dwangmiddelenrechtbank[203] ('*Zwangsmaßnahmengericht*') vereist.[204] Deze rechter is vergelijkbaar met de rechter-commissaris in Nederland. De autorisatie moet er onder andere voor zorgen dat betrokkenen beschermd worden tegen mogelijk misbruik van GovWare.[205] De controle door deze rechtbank vindt plaats *nadat* het Openbaar Ministerie de maatregel heeft ingesteld (*ex post*) (Godenzi & Caprara, 2018, p. 299). Binnen 24 uur na afgifte van het bevel dient de officier van justitie bij de dwangmiddelenrechtbank het bevel in, inclusief een onderbouwing voor de inzet en de zaaksdocumenten die relevant zijn voor het nemen van een beslissing door de dwangmiddelenrechtbank.[206] Binnen vijf dagen nadat een bevel is afgegeven neemt de dwangmiddelenrechtbank een beslissing en licht zij deze toe. Het is mogelijk om aan de toestemming voor de inzet van de bevoegdheid een tijdslimiet te verbinden of om nadere informatie en onderzoek te vragen.[207] De dwangmiddelenrechtbank brengt de

198 Dit zou al logisch voorvloeien uit het feit dat de persoon bij wie de doorzoeking wordt gedaan (art. 247 Sv) geïnformeerd dient te worden. Het informeren van een verdachte is bij het gebruik van GovWare niet aan de orde. De inzet van Govware zou dan immers geen zin meer hebben (Botschaft, 27 februari 2013, p. 2779).
199 Botschaft 27 februari 2013, p. 2702; p. 2776; p. 2779. Betschamnn & Murer Mikolásek (2018) beschrijven dat er discussie bestaat of het een mogelijkheid is om de artikelen 269ter en 280 Sv gecombineerd in te zetten zodat toch een microfoon of een camera zouden mogen worden aangezet. Volgens beide auteurs is dat niet mogelijk, omdat dit ook betrekking kan hebben op het opnemen van privécommunicatie die niets te maken heeft met telecommunicatieverkeer (Betschamnn & Murer Mikolásek, 2018, p. 751).
200 Artikel 269ter lid 3 Sv; artikel 141 lid 1 Sv; artikel 277 Sv; Botschaft, 27 februari 2013, p. 2776.
201 Artikel 16 Sv en artikel 7 wet op de rechterlijke organisatie (StBOG).
202 Artikel 269ter lid 1 Sv.
203 Bij heimelijke bevoegdheden moet het Openbaar Ministerie meestal toestemming vragen aan een rechter (Godenzi & Caprara, 2018, p. 301).
204 Artikel 272 lid 1 Sv.
205 Botschaft 27 februari 2013, p. 2776.
206 Artikel 274 lid 1a en 1b Sv.
207 Artikel 274 lid 2 Sv.

officier van justitie en het post- en telecommunicatie surveillance bureau in de zin van artikel 3 BÜPF direct op de hoogte van de genomen beslissing.[208] In de beslissing wordt vastgelegd welke maatregelen genomen moeten worden om beroepsgeheimen te beschermen en of niet-openbare plaatsen betreden mogen worden om GovWare te installeren.[209]

Een officier van justitie geeft uiteindelijk een bevel aan de politie (kanton of federaal). In Zwitserland is de aanschaf en het gebruik van GovWare gecentraliseerd (EJPD, 2019b, p. 2). In één van de interviews komt naar voren dat ook de politie in de kantons deze bevoegdheid zou moeten kunnen toepassen, maar dat kennis hierover ontbreekt. In de praktijk biedt de federale politie GovWare aan, beheert zij de licenties, neemt zijn het onderhoud voor haar rekening en ondersteunt zij de verschillende kantons. Ook is de federale politie contactpersoon voor de fabrikant (EJPD, 2019b, p. 2). Als een kanton gebruik wil maken van GovWare (en er is toestemming), dan betaalt dit kanton per maand een bedrag aan de federale politie. De exacte bedragen[210] zijn vastgelegd in artikel 3a van de Verordening (Fedlex, 2017) en de toelichting op deze verordening. De federale politie beschikt over acht licenties (geschikt voor acht geautomatiseerde werken) die tegelijkertijd kunnen worden ingezet (EJPD, 2019b, p. 4). De federale politie verzamelt de gegevens met behulp van GovWare en draagt deze daarna over aan het politieteam dat het opsporingsonderzoek uitvoert.[211]

7.3 Tegen wie

De bevoegdheid mag worden ingezet tegen een verdachte,[212] maar ook tegen derden. Aan dat laatste zijn wel voorwaarden verbonden: (1) de verdachte maakt gebruik van het postadres of de telecommunicatiedienst van een derde partij;[213] òf (2) de derde partij ontvangt of stuurt communicatie door namens de verdachte.[214]
Indien surveillance plaatsvindt van een geheimhouder[215] wordt informatie die geen verband houdt met het onderwerp van onderzoek geheim gehouden onder leiding van een rechter. Dat geldt ook voor de reden waarom die persoon wordt geobserveerd. Er mogen geen beroepsgeheimen ter kennis komen van het Openbaar Ministerie. De gescheiden gegevens dienen onmiddellijk te worden vernietigd en zij mogen niet worden geanalyseerd.[216] Informatie hoeft niet te worden gescheiden als (1) een sterk vermoeden bestaat dat de geheimhouder een strafbaar feit heeft gepleegd;[217] en (2) bijzondere reden dit vereisen.[218] Indien surveillance plaatsvindt van andere personen en zij hebben contact met personen zoals bedoeld in de artikelen 170-173 Sv, dan wordt die communicatie overeenkomstig lid 1 gescheiden. De informatie waarover

[208] Artikel 274 lid 3 Sv.
[209] Artikel 274 lid 4 Sv.
[210] Eén maand kost 13.750 Zwitserse francs, twee maanden 27.500 Zwitserse francs en drie maanden 41.250 Zwitserse francs. Indien een inzet verlengd wordt, dan wordt daarvoor een apart bedrag in rekening gebracht (EJPD, 2019b, p. 4).
[211] Dit onderscheid tussen techniek en tactiek wordt ook gemaakt bij de Nederlandse politie (Van Uden & Van den Eeden, 2022).
[212] Artikel 270 lid a Sv.
[213] Artikel 270 lid b, paragraaf 1 Sv.
[214] Artikel 270 lid b, paragraaf 2 Sv. Volgens jurisprudentie wordt surveillance van telecommunicatie ook toegestaan indien het zeer waarschijnlijk is dat de derde communicatie van de verdachte ontvangt (BGE 138 IV 232).
[215] Een persoon die behoort tot een beroepsgroep zoals bedoeld in de artikelen 170-173 Sv (onder andere personen die ambtsgeheim hebben of een beroepsgeheim hebben zoals advocaten en artsen).
[216] Artikel 271 lid 1 Sv.
[217] Artikel 271 lid 2a Sv.
[218] Artikel 271 lid 2b Sv.

een persoon zoals bedoeld in de artikelen 170-173 Sv kan weigeren te getuigen, wordt gescheiden van het procesdossier en onmiddellijk vernietigd. Die informatie mag niet worden gebruikt.[219]

7.4 Gevallen

Govware kan worden gebruikt voor diverse misdrijven zoals opzettelijke doodslag (art. 111 Sr), moord (art. 112 Sr), verduistering (art. 138 Sr.), fraude (art. 147 lid 1 en 2 Sr), mensenhandel (art. 182 Sr) en deelname aan een criminele en terroristische organisatie (art. 260ter Sr). Artikel 269ter lid 1b Sv regelt dat GovWare kan worden gebruikt voor misdrijven die staan opgesomd in artikel 286 lid 2 Sv.[220] Het gaat daarbij niet alleen om misdrijven genoemd in het Wetboek van Strafrecht (‘*Schweizerisches Strafgesetzbuch*’), maar ook om misdrijven die in andere wetten[221] zijn opgenomen.[222]

7.5 Termijn

De dwangmiddelenrechtbank geeft in eerste instantie toestemming voor een periode van maximaal drie maanden. Daarna kan een inzet eenmaal of meerdere keren worden verlengd, steeds met een periode van maximaal drie maanden. Er is geen maximale periode of maximaal aantal verlengingen afgesproken. Indien een officier van justitie wil dat de inzet verlengd wordt dan dient hij/zij hiervoor een aanvraag in bij de dwangmiddelenrechtbank waarin beargumenteerd wordt waarom de inzet verlengd dient te worden. Deze aanvraag moet bij de rechtbank worden ingediend vóór de einddatum van de inzet waarvoor eerder al toestemming was gegeven.[223] Op het moment dat niet meer aan de voorwaarden voor een inzet kan worden voldaan[224] of wanneer geen toestemming wordt gegeven voor de inzet of voor de verlenging, beëindigt een officier van justitie de inzet direct.[225] Indien sprake is van een situatie zoals bedoeld in lid 1a, zal de officier van justitie de dwangmiddelenrechtbank op de hoogte brengen van de beëindiging van de inzet.[226]

7.6 Formaliteiten

De voorwaarden voor de inzet van GovWare staan opgesomd in artikel 269 lid 1 en 3.[227] Het gaat om het volgende: (a) er een dringende verdenking is dat een misdrijf is gepleegd dat staat genoemd in lid 2 van het betreffende artikel; (b) de ernst van het misdrijf surveillance rechtvaardigt; en (c) onderzoeksactiviteiten die tot dan toe zijn

[219] Artikel 271 lid 3 Sv.
[220] Dit laatste artikel heeft betrekking op infiltratie.
[221] Bijvoorbeeld de Federale wet van 22 juni 2001 aangaande de Haagse conventie over adoptie en maatregelen om kinderen te beschermen in internationale adoptiezaken (‘Bundesgesetz vom 22. Juni 2001133 zum Haager Adoptionsübereinkommen und über Massnahmen zum Schutz des Kindes bei internationalen Adoptione’), de Wapenwet (‘Waffengesetz vom 20. Juni 1997’) en de Wet verdovende middelen (‘Betäubungsmittelgesetz vom 3. Oktober 1951’).
[222] Op basis van artikel 269ter lid 1a Sv zou verondersteld kunnen worden dat GovWare ook gebruikt mag worden in het geval van de misdrijven die staan opgesomd in artikel 269, lid 2 Sv. In de toelichting op de revisie van de BÜPF staat echter beschreven dat artikel 269ter, lid 1a Sv niet verwijst naar artikel 269 lid 2 Sv. Ondermeer vanwege de ingrijpendheid van de bevoegdheid.
[223] Artikel 274 lid 5 Sv.
[224] Artikel 275 lid 1a Sv.
[225] Artikel 275 lid 1b Sv.
[226] Artikel 275 lid 2 Sv.
[227] Artikel 269 Sv regelt de surveillance van post- en telecommunicatie.

uitgevoerd geen resultaat hebben opgeleverd of het onderzoek anders zinloos of onevenredig moeilijk zou zijn.[228] Lid 3 beschrijft dat de surveillance van post en telecommunicatie kan worden bevolen wanneer de berechting van een strafbaar feit, dat onder militaire rechtsmacht valt, opgedragen wordt aan een civiele rechtbank. Naast deze voorwaarden moet, voordat overgegaan wordt tot de inzet van de bevoegdheid, eerdere 'traditionele' surveillance van telecommunicatie (art. 269 Sv) niet succesvol zijn geweest. Ook kan de bevoegdheid worden ingezet wanneer deze traditionele vorm van surveillance nutteloos of onevenredig moeilijk is (art. 269ter lid 1c Sv).[229] De bevoegdheid mag verder alleen in opsporingsonderzoeken ('*Straf-verfahren*') worden gebruikt en niet preventief worden ingezet.[230]
Indien de officier van justitie een bevel afgeeft voor de inzet van de bevoegdheid, moet daarin de volgende informatie zijn opgenomen: de soorten gegevens en niet-publieke ruimtes die mogelijk betreden moeten worden om de software te installeren op het geautomatiseerd werk.[231]

Opnames, waarvoor toestemming was om die te genereren, maar die niet nodig zijn in het strafproces, moeten apart van het dossier bewaard worden en direct na afloop van het proces verwijderd worden.[232] Artikel 278 Sv richt zich op toevalsbevindingen. Het gaat onder andere over de wijze waarop moet worden omgegaan met gegevens die worden verzameld en die betrekking hebben op andere strafbare feiten dan waarvoor een bevel was afgegeven en de omstandigheden waaronder deze kunnen worden gebruikt.[233] In lid 5 is geregeld dat alle bevindingen kunnen worden gebruikt voor het opsporen van personen die gezocht worden. Verder is nog geregeld dat gegevens die verzameld worden met behulp van de software en die niet in het bevel staan opgenomen direct vernietigd dienen te worden. Er mag geen gebruik worden gemaakt van informatie die afkomstig is uit die gegevens.[234] Tot slot is in artikel 269ter Sv opgenomen dat de officier van justitie statistieken bij zal houden van de inzet van deze bevoegdheid. Meer hierover is geregeld in artikel 13 van de Verordening betreffende het toezicht op het post- en telecommunicatieverkeer ('*Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*' (VÜPF).[235]

7.7 Technische hulpmiddelen

Zoals eerder genoemd voert de federale politie de werkzaamheden uit met betrekking tot GovWare. In één van de interviews wordt aangegeven dat de politie zowel zelf ontwikkelde als commerciële tools gebruikt. De federale politie zorgt er, na een bevel van de officier van justitie, voor dat de software op het geautomatiseerd werk van de verdachte wordt geplaatst. Dat kan zowel fysiek als op afstand gebeuren. Afhankelijk van het bevel van de officier van justitie wordt de software afgestemd op (ontworpen voor) het geautomatiseerd werk van de verdachte en geconfigureerd. Tijdens de dataverzameling worden de onderschepte gegevens via de telecommunicatieverbinding van de verdachte naar de server van het Openbaar Ministerie en de politie

[228] Artikel 269 lid 1 Sv.
[229] Artikel 269ter lid 1c Sv heeft overeenkomsten met artikel 269 lid 3 Sv.
[230] Botschaft 27 februari 2013, p. 2701; p. 2771.
[231] Artikel 269ter lid 2a en 2b Sv.
[232] Artikel 276 Sv lid 1 Sv.
[233] Artikel 278 lid 1.
[234] Artikel 269ter lid 3 Sv.
[235] Voor de inzet van dwangmaatregelen in het algemeen geldt ook een aantal 'standaard' voorwaarden. Deze staan vastgelegd in artikel 197 CCP. In lid 1b van dat artikel is bijvoorbeeld geregeld dat voor de inzet van een dwangmaatregel er een redelijke verdenking moet zijn dat een misdrijf is gepleegd.

(‘*Strafverfolgungsbehörden*’) gestuurd.[236] De software dient zodanig geconfigureerd te worden dat alleen communicatiegegevens onderschept kunnen worden. Daarmee wordt voorkomen dat ook een online doorzoeking mogelijk is. GovWare moet zo zijn geconfigureerd dat de ontwikkelaar van GovWare geen toegang heeft tot de gegevens als het technisch hulpmiddel wordt gebruikt. Ditzelfde geldt voor personen die vanuit de politie betrokken zijn bij het beheer van GovWare, bijvoorbeeld iemand die de server beheert waarop de gegevens worden opgeslagen verkregen met GovWare.

Omdat de software aangepast wordt aan het apparaat van de verdachte, en de software niet lang op het geautomatiseerd werk staat, zou het zeer moeilijk zijn de software te kopiëren en op een ander apparaat te plaatsen. Een derde zou de software dus niet gemakkelijk kunnen misbruiken.[237] Indien de gegevensverzameling beëindigd wordt, zorgt de politie voor het deactiveren van GovWare. Dit laatste is niet nodig wanneer deactivatie automatisch plaatsvindt.[238] In de toelichting op de nieuwe wet wordt nog opgemerkt dat geraadpleegde experts uit de wetenschap menen dat de software die gebruikt zou worden nog niet beperkt kan worden tot enkel het onderscheppen van communicatie. Er zou toegang kunnen worden verkregen tot alle gegevens die op een geautomatiseerd werk staan.[239]

7.8 Waarborgen

7.8.1 Volledige vastlegging & veilig versturen gegevens

Gedurende het wetgevingstraject hebben providers en diverse particuliere individuen zorgen geuit over de kwaliteit van de gegevens die worden verzameld met behulp van GovWare, meer in het bijzonder over de betrouwbaarheid en de integriteit van die gegevens (de mogelijke wijzigingen die GovWare in documenten aanbrengt).[240] In het Zwitserse Wetboek van Strafvordering is uiteindelijk een beperkt aantal voorwaarden opgenomen dat betrekking heeft op de kwaliteit van GovWare en de kwaliteit van de gegevens die met behulp van deze software verzameld worden. In artikel 269quater Sv staan deze voorwaarden beschreven. De eerste voorwaarde is dat alleen software mag worden gebruikt die ‘onveranderlijk en zonder onderbreking’ communicatie vastlegt.[241] De tweede voorwaarde is dat het versturen van gegevens van het geautomatiseerd werk van de verdachte naar de politie en het Openbaar Ministerie (‘*Strafverfolgungsbehörde*’) veilig moet verlopen.[242] Voor beide voorwaarden geldt dat in de wet niets is vastgelegd over de wijze waarop die voorwaarden gegarandeerd en gerealiseerd zouden moeten worden. Ook bestaat er geen openbare politierichtlijn waarin deze voorwaarden naar technische eisen vertaald worden.[243] Wel wordt uit

[236] Botschaft 27 februari 2013, p. 2774.
[237] Botschaft 27 februari 2013, p. 2774-2775.
[238] Botschaft 27 februari 2013, p. 2774.
[239] Botschaft 27 februari 2013, p. 2775.
[240] Botschaft 27 januari 2013, p. 2773.
[241] Art. 269quater, lid 1 Sv.
[242] Art. 269quater, lid 2 Sv.
[243] Voor het onderscheppen van post en telecommunicatie bestaan diverse aanvullende wetten en verordeningen, zoals de BÜPF, VÜPF, VBO-ÜPF (*Verordnung des EJPD über das beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs*), Gebv-ÜPF (*Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs*), VD-ÜPF (*Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs*) en VVS-ÜPF (*Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs*). Behalve artikel 13 VÜPF, waarin geregeld wordt dat het Openbaar Ministerie statistieken bij dient te houden over het gebruik van GovWare, hebben deze aanvullende wetten en verordeningen geen betrekking op de inzet van GovWare. Artikel 13 VÜPF regelt dat uit de cijfers moet blijken voor welk type misdrijf deze bevoegdheid is ingezet (art. 13, lid 1 BÜPF). Deze statistieken zullen vervolgens worden voorgelegd aan de Post en Telecommunicatie Surveillance Dienst. Het gaat daarbij om inzetten die afgerond zijn (art. 13, lid 2 VÜPF). Deze dienst

interviews duidelijk dat de politie GovWare test aan de hand van een aantal voorwaarden en dat maatregelen genomen worden om gegevens veilig te kunnen versturen, bijvoorbeeld hashing en het werken met forensische containers.[244] Ook wordt aangegeven dat in een verslag aan de officier van justitie uiteen wordt gezet hoe er gewerkt is, inclusief de hashes. Wat dat laatste betreft wordt door een geïnterviewde aangegeven dat het Openbaar Ministerie en de rechtbank de politie vertrouwen. Tegelijkertijd wordt aangegeven dat, mocht er enige twijfel zijn over het bewijs dat gepresenteerd wordt, het Openbaar Ministerie en de rechter zeker zullen willen weten dat het bewijs op een rechtmatige manier verzameld is. Indien blijkt dat dat niet het geval is, dan moet de toelaatbaarheid worden getoetst aan de beginselen die vastgelegd zijn in artikel 140 Sv ('Verboden methoden van bewijsverzameling', bijvoorbeeld dreiging en het gebruik van geweld). Artikel 141 Sv gaat vervolgens in op de toelaatbaarheid van bewijs dat niet rechtmatig verkregen is (persoonlijke communicatie, 31 maart 2023). Bewijs dat verzameld is met behulp van geweld mag bijvoorbeeld niet worden gebruikt.[245]

7.8.2 Openbaarmaking broncode

De derde voorwaarde is dat de justitiële autoriteiten moeten kunnen verzekeren dat de broncode gecontroleerd kan worden zodat met zekerheid kan worden gesteld dat de software alleen beschikt over de wettelijk toegestane functies (art. 269quater, lid 3 Sv). In één van de interviews wordt uitgelegd dat commerciële leveranciers schriftelijk moeten bevestigen dat zij akkoord zijn met het prijsgeven van de broncode, als een rechtbank daar om vraagt. Voor zover bekend is zo'n verzoek tot openbaarmaking tot nu toe (nog) niet gedaan.

7.8.3 Speciale dienst en keuring

In het oorspronkelijke wetsvoorstel waren nog twee voorwaarden opgenomen (Basanisi, 2019, p. 12). De eerste was dat de Zwitserse Bondsstaat ('*der Bund*') een dienst zou gaan beheren die speciale IT-programma's aanschaft. Deze dienst zou de taak hebben om computerprogramma's te ontwikkelen om communicatie te monitoren of om deze programma's bij derden in te kopen. De tweede voorwaarde was dat alleen programma's zouden mogen worden gebruikt die door de Bondstaat goedgekeurd zijn. Dit impliceert dat de Bondstaat keuringen zou gaan uitvoeren. Ook zou een redelijke vergoeding worden betaald voor de kosten van de aanschaf van speciale programma's. Uiteindelijk zijn deze voorwaarden, na een beslissing in januari 2016 van de juridische Commissie van de Nationale Raad over de herziening van de BÜPF ('*der Rechtskommission des Nationalrates zur Revision des BÜPF*'), niet opgenomen in de wet (Basanisi, 2019, p. 12-13). Verschillende argumenten speelden een rol om voorafgaande certificering en de centrale aanschaf van GovWare niet te willen opnemen in de wet. De commissie achtte bijvoorbeeld voorafgaande certificering problematisch, omdat software continu (wekelijks) geüpdatet moet worden. Dat zou betekenen dat bij elke nieuwe update nieuwe certificering vereist is en dat software die een update heeft ondergaan niet direct kan worden gebruikt. Om tot certificering te komen, zal immers eerst getest dienen te worden. Daarnaast zou certificering veel tijd, inspanning en middelen vergen, denk aan de controle van enkele honderdduizenden regels code. Door certificering zouden de kosten van dit soort programma's verschillende keren

zal de cijfers jaarlijks publiceren. Er worden geen details prijsgegeven over het kanton van de autoriteit die om de inzet van de bevoegdheid verzocht (art. 13, lid 3 VÜPF).

[244] Uitgelegd wordt ook dat voor de politie niet volledig duidelijk is wat er gebeurt wanneer de gegevens het toestel verlaten en verstuurd worden naar de politie-omgeving.

[245] Artikel 141 lid 1 Sv.

stijgen. Daarnaast meende de commissie dat het centraal aanschaffen problematisch is, omdat het de vraag is wie uiteindelijk verantwoordelijk is als GovWare schade veroorzaakt aan een geautomatiseerd werk (de federale staat of de kantons zelf) (Engler, 2015). Sommige van deze punten (ontwikkeling, aanschaf en kosten) vastgelegd in een verordening (zie eerder).

7.8.4 Andere technische en organisatorische maatregelen

Op haar overheidswebsite beantwoordt het federale departement van politie en justitie (EJPD, 2023) (‘*Eidgenössischen Justiz- und Polizeidepartements*’) een aantal vragen over het monitoren van telecommunicatie die te maken hebben met de kwaliteit van de gegevens die verzameld worden. De EJPD geeft aan dat, voor een zo veilig mogelijk gebruik van GovWare, zowel technische als organisatorische maatregelen zullen worden genomen. Wat betreft technische maatregelen moeten de politie en het Openbaar Ministerie (‘*Strafverfolgungsbehörden’*) de noodzakelijke beveiligingsfuncties formuleren. Vervolgens controleert een onafhankelijke instantie of deze volledig zijn en ingebouwd zijn volgens de erkende normen. In het kader van organisatorische maatregelen zullen de politie en het Openbaar Ministerie een gedetailleerd proces beschrijven voor het gebruik en de werking van GovWare. Het gaat hierbij onder andere om autorisaties en de omgang met het geautomatiseerde werk. Verder moet logging ervoor zorgen dat alle stappen (vanaf het moment van aanvraag tot en met de monitoring) traceerbaar zijn, ook voor de rechtbank (EJPD, 2023). De zojuist genoemde punten zijn niet vastgelegd in de wet. Daarnaast is het onduidelijk of er uiteindelijk een onafhankelijke instantie is gekomen en in hoeverre de andere maatregelen zoals bijvoorbeeld het vastleggen van autorisaties en logging in de praktijk worden nageleefd. Hierover bestaat geen openbare informatie. Wel wordt in één van de interviews aangegeven dat er wordt gelogd, maar dat het daarbij niet gaat om technische logging, maar om het laten zien welke gegevens zijn binnengehaald (dat dit bijvoorbeeld alleen de gegevens waren waarvoor de officier van justitie toestemming had gegeven). Wat wordt gelogd, zouden politie en de officier van justitie met elkaar afstemmen.

7.8.5 Verslaglegging en dossier

Artikel 76 Sv kent een aantal algemene bepalingen wat schriftelijk dient te worden vastgelegd. Het gaat bijvoorbeeld om verklaringen, mondelinge beslissingen van de autoriteiten en alle andere proceshandelingen die niet schriftelijk worden verricht (art. 76 lid 1 Sv). Dit artikel heeft geen betrekking op politierapporten. Dat wordt geregeld in artikel 306 Sv lid 1, waarin is vastgelegd dat de politie met behulp van processen-verbaal relevante feiten vaststelt, aanwijzingen van de officier van justitie of eigen vaststellingen. Bij haar werkzaamheden laat de politie zich leiden door bepalingen die gaan over opsporing, bewijs en dwangmiddelen, bijvoorbeeld met betrekking tot dagvaardingen (art. 206 Sv) en arrestaties (art. 217 Sv). Bijzondere bepalingen van deze wet zijn voorbehouden (art. 306 Sv lid 3). In één van de interviews komt naar voren dat de politie na afloop van de inzet voor de officier van justitie een verslag schrijft wat er in het kader van de uitvoering van de bevoegdheid gedaan is. Er wordt onder andere aandacht besteed aan het gegeven dat er gegevens zijn opgehaald, dat die opgeslagen zijn en dat ze zijn gehasht. Over de exacte werkwijze van technische maatregelen (zoals GovWare) wordt geen informatie openbaar gemaakt. Het verslag komt in het dossier. Verder geldt als algemene regel dat partijen inzage kunnen krijgen in het dossier van de strafprocedure. Uiterlijk na het eerste verhoor van de verdachte en het verzamelen van andere belangrijke bewijsmiddelen door het

Openbaar Ministerie is dit mogelijk (art. 101 CCP). Uit de jurisprudentie volgt dat verdachten het recht hebben om inzage te krijgen in de opnames van communicatie zodat zij zich een beeld kunnen vormen van de wijze waarop de autoriteiten opnames geselecteerd hebben (Bundesgericht, 2019). Omdat de hackbevoegdheid onderdeel is van de bevoegdheid tot het onderscheppen van communicatie zou deze jurisprudentie ook betrekking hebben op gegevens die verzameld worden middels de hackbevoegdheid (persoonlijke communicatie, 1 mei 2023).

7.8.6 Notificatieplicht

Uiterlijk nadat het vooronderzoek is beëindigd, brengt de officier van justitie een verdachte op de hoogte van de inzet van de bevoegdheid.[246] Aan de verdachte dient te worden medegedeeld wat de reden was voor de inzet en wat de aard van de inzet en de looptijd waren. Indien de dwangmiddelenrechtbank hiervoor toestemming geeft, kan notificatie achterwege worden gelaten. Dat is toegestaan in twee gevallen:
(1) wanneer bevindingen niet gebruikt zullen worden voor bewijsdoeleinden;[247] of
(2) wanneer uitstel of het achterwege laten van notificatie noodzakelijk is om hogere publieke of particuliere belangen te beschermen.[248] Personen tegen wie deze bevoegdheid is ingezet, kunnen bezwaar maken op basis van de artikelen 393-397 Sv. De termijn waarbinnen bezwaar kan worden ingediend start op het moment dat genotificeerd is.[249]

7.9 Jurisprudentie

Zoals eerder vermeld dient jaarlijks bekend te worden gemaakt hoe vaak GovWare is ingezet. In 2020 is dertien keer gebruikgemaakt van GovWare en in 2021 elf keer (EJPD, 2022). Voor zover bekend zijn er geen openbare uitspraken over zaken waarin GovWare op basis van artikel 269ter Sv is toegepast. Eén van de geïnterviewden geeft aan op de hoogte te zijn van twee of drie zaken waarin gegevens verzameld met behulp van GovWare naar voren zijn gebracht èn (zonder discussie) zouden zijn geaccepteerd. Omdat in deze zaken hoger beroep is aangetekend, konden de uitspraken niet met de onderzoekers worden gedeeld. In een ander interview komt naar voren dat er aanwijzingen zijn dat GovWare op basis van artikel 280 Sv is ingezet. Voor zover bekend is ook voor het gebruik van GovWare op basis van artikel 280 Sv geen jurisprudentie beschikbaar.

7.10 Tot slot

Op basis van artikel 269ter Sv kan in Zwitserland in een opsporingsonderzoek gebruik worden gemaakt van GovWare om communicatiegegevens en metagegevens te onderscheppen. Op die manier is het voor de politie mogelijk om inzicht te krijgen in versleutelde communicatie. GovWare mag niet worden ingezet voor een online doorzoeking. Ook zou het niet zijn toegestaan om GovWare te gebruiken voor observaties, bijvoorbeeld door met behulp van GovWare de camera in een geautomatiseerd werk aan te zetten.

[246] Artikel 279 lid 1 Sv.
[247] Artikel 279 lid 2a Sv.
[248] Artikel 279 lid 2b Sv.
[249] Artikel 279 lid 3 Sv.

In de wet zijn drie voorwaarden vastgelegd die de kwaliteit van de verzamelde gegevens ten goede zou moeten komen. Deze hebben zowel betrekking op de periode voorafgaand aan de inzet, tijdens de inzet van de bevoegdheid als na afloop van de inzet. De eerste voorwaarde is dat alleen software mag worden gebruikt die 'onveranderlijk en zonder onderbreking' communicatie vastlegt. De tweede voorwaarde is dat het versturen van gegevens van het geautomatiseerd werk van de verdachte naar de justitiële autoriteiten veilig moet verlopen. De derde voorwaarde is dat de gebruikte broncode openbaar moet kunnen worden gemaakt, zodat kan worden aangetoond dat de software niet over meer functionaliteiten beschikt dan wettelijk is toegestaan. Twee voorwaarden zijn uiteindelijk niet opgenomen in de definitieve versie van de wet: er komt een aparte dienst die software ontwikkelt en aanschaft en onderzoeksrechters mogen alleen technische hulpmiddelen gebruiken die door de Bondsraad zijn goedgekeurd.

In het kader van het waarborgen van de kwaliteit van de verzamelde gegevens, springen drie punten in het oog. In de eerste plaats is in de wet zelf of in nadere aanvullende regelingen (zoals bijvoorbeeld in Nederland in het Besluit) niets vastgelegd over de concrete invulling van voorwaarden die in de wet genoemd worden. Op een FAQ-website van de overheid wordt een aantal van deze punten wel wat meer concreet gemaakt. Zo geeft het federaal departement van politie en justitie aan dat de politie en het Openbaar Ministerie zelf beveiligingseisen moeten formuleren en dat er een onafhankelijke instantie moet komen die deze eisen controleert. Ook wordt aangegeven dat autorisaties vastgelegd dienen te worden en dat dit gelogd dient te worden. Er is echter geen openbare informatie beschikbaar over de invulling van deze eisen, of een dergelijke onafhankelijke instantie in het leven geroepen is en of er alleen gewerkt kan worden met goedgekeurde technische hulpmiddelen. In de praktijk beoordeelt de federale politie zelf GovWare die zij inzet en bepaalt zij zelf, in overleg met het Openbaar Ministerie, welke maateregelen zij neemt om de kwaliteit van de gegevens te waarborgen en wat er wordt vastgelegd. In dat opzicht is er vanuit het Openbaar Ministerie in principe het vertrouwen dat de politie het goede doet. Op dit moment is nog geen jurisprudentie beschikbaar op basis waarvan beoordeeld zou kunnen worden of dat in de ogen van de rechter inderdaad het geval is (en of de door de politie gekozen en verantwoorde methoden volstaan).

Een tweede punt dat opvalt heeft te maken met het beschikbaar stellen van de broncode. Op papier lijkt dat een mooie methode om meer inzicht te krijgen in de precieze werking van de gebruikte GovWare. Bedrijven die GovWare leveren aan de Zwitserse politie zouden ook toegestemd hebben om die broncode beschikbaar te stellen als de rechter daar om vraagt. In de praktijk is het echter de vraag of die broncode uiteindelijk beschikbaar zal komen. Basanisi (2018, p. 14-15) is hier sceptisch over. Zo merkt hij op dat het problematisch is dat het begrip broncode niet nader gedefinieerd is. Volgens hem is goede controle alleen mogelijk als de broncodes van de programma's worden vrijgegeven die verantwoordelijk zijn voor zowel het binnendringen als voor het monitoren van de gegevens die op het geautomatiseerd werk staan. Verder vraagt Basanisi (2019, p. 14-15) zich af of controle van de broncode praktisch uitvoerbaar is. Hij heeft aanwijzingen dat in de praktijk de broncode niet beschikbaar wordt gesteld (Basanisi, 2018, p. 14-15). Uit eerder onderzoek van het WODC komt naar voren dat in Nederland dit in de praktijk ook lastig bleek. Tenminste één leverancier was niet bereid om inzicht te geven in de precieze werking van het product (Van Uden & Van den Eeden, 2022, p. 99). Omdat in Zwitserland, voor zover bekend, geen jurisprudentie beschikbaar is met betrekking tot

zaken waarin GovWare is gebruikt, kan de vraag of de broncode uiteindelijk beschikbaar wordt gesteld, (nog) niet definitief beantwoord worden.

Een derde punt tot slot, heeft betrekking op de informatieverstrekking aan de verdachte en de verdediging. Zwitserland kent een notificatieplicht waarin een verdachte op de hoogte wordt gesteld dat de bevoegdheid is ingezet (hierop zijn uitzonderingen mogelijk). Ook legt de politie in een proces-verbaal vast welke handelingen zij heeft verricht en welke beveiligingsmaatregelen zijn genomen. Er wordt geen beschrijving gegeven van de exacte werking van het technisch hulpmiddel. Deze informatieverstrekking biedt de verdediging van de verdachte in principe de mogelijkheid om vragen te stellen over de kwaliteit van de gegevens. In hoeverre dat in de praktijk daadwerkelijk gebeurt, en of de verdediging hiertoe voldoende informatie beschikbaar heeft, is tijdens dit onderzoek niet duidelijk geworden.

8 Conclusie

Een belangrijke aanleiding voor dit rechtsvergelijkend onderzoek was het eerste Verslag van de Inspectie Justitie & Veiligheid (hierna Inspectie) in 2020. Op basis daarvan concludeerde de toenmalig Minister van Justitie en Veiligheid dat de inzet van technische hulpmiddelen bij de hackbevoegdheid en de keuring van deze hulpmiddelen nog niet verliepen zoals volgens het wettelijk kader was bedoeld. Ook in het evaluatie-rapport over de uitvoering van de hackbevoegdheid in de praktijk, uitgevoerd door het WODC, komt eenzelfde beeld naar voren. In zijn reactie op het eerste Verslag van de Inspectie heeft de minister aangegeven dat hij zou laten onderzoeken met welke waarborgen het gebruik van technische hulpmiddelen in het buitenland is omkleed. Onderhavig rapport is het resultaat van dit onderzoek.

De centrale onderzoeksvraag van dit onderzoek was als volgt:

Met welke waarborgen is in het buitenland de hackbevoegdheid, meer in het bijzonder het gebruik van technische hulpmiddelen, omkleed en hoe verhoudt zich dat tot de Nederlandse situatie?

Om de onderzoeksvraag te beantwoorden zijn verschillende onderzoeksmethoden gebruikt: documentstudie (wet- en regelgeving en relevante (grijze) literatuur), schriftelijke vragenlijsten en interviews. Op basis hiervan is een brede inventarisatie gemaakt van een groot aantal Europese landen en Australië, Canada en de Verenigde Staten. Daarnaast zijn vijf landen – België, Duitsland, Frankrijk, Zweden en Zwitserland – meer diepgaand bestudeerd. Een analyse van de Nederlandse situatie had al plaatsgevonden in het kader van de eerdergenoemde evaluatie naar de uitvoering van de hackbevoegdheid in de praktijk.

In deze conclusie worden vijf landen die meer diepgaand bestudeerd zijn met elkaar en met Nederland vergeleken. In paragraaf 8.1 wordt eerst kort ingegaan op de belangrijkste (knel-)punten in Nederland ten aanzien van de keuring van technische hulpmiddelen. Vervolgens wordt in paragraaf 8.2 ingegaan op een aantal algemene observaties met betrekking tot het buitenland, gebaseerd op de brede inventarisatie die is uitgevoerd. In paragraaf 8.3 worden de landen vergeleken die diepgaander bestudeerd zijn. Paragraaf 8.4 bevat een slotbeschouwing waarin wij een aantal scenario's voor Nederland verkennen die gaan over (aanvullende) waarborgen ten aanzien van de kwaliteit van de gegevens verkregen middels de hackbevoegdheid. Deze scenario's zijn gebaseerd op de manier waarop de verschillende buitenlanden met de hackbevoegdheid omgaan.

8.1 Belangrijkste (knel)punten keuring technische hulpmiddelen in Nederland

De Nederlandse wetgever heeft ervoor gekozen om bij de introductie van de hackbevoegdheid het keuringssysteem van technische hulpmiddelen te volgen dat gebruikt wordt voor al bestaande (bijzondere) opsporingsbevoegdheden. Voor de hackbevoegdheid is een apart besluit genaamd 'Besluit onderzoek in een geautoma-tiseerd werk' (hierna Besluit) ontworpen. In dit Besluit worden diverse eisen gesteld aan een technisch hulpmiddel, waaronder eisen die gericht zijn op de integriteit, herleidbaarheid en betrouwbaarheid (hierna kwaliteit) van de verzamelde gegevens.

De Keuringsdienst voert de keuringen in Nederland uit en zij hanteert daarbij een keuringsprotocol dat gebaseerd is op diverse artikelen uit het Besluit. In principe moet de politie gebruikmaken van een technisch hulpmiddel dat vooraf (goed-)gekeurd is. Hiervoor geldt een aantal uitzonderingen: (1) een technisch hulpmiddel kan achteraf gekeurd worden; (2) er kan worden overgegaan op een handmatige inzet; of (3) de officier van justitie oordeelt dat het middel 'naar zijn aard' niet te keuren is.

Uit de Verslagen van de Inspectie (Inspectie JenV, 2020; 2021; 2022) en het eerste evaluatierapport van het WODC (Van Uden & Van den Eeden, 2022) blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk bedoeld. Het inzetten van een vooraf goedgekeurd technisch hulpmiddel gebeurt niet of nauwelijks en voor de opsporingspraktijk vormt de keuring een belangrijk knelpunt. Verschillende aspecten spelen hierbij een rol (Van Uden & Van den Eeden, 2022, p. 131-147):

- De doorlooptijd van een keuring neemt relatief veel tijd in beslag, tenminste vier maanden. Die tijd past niet altijd bij de snelheid die nodig kan zijn binnen een opsporingsonderzoek.
- Een technisch hulpmiddel aanpassen dat nog niet goedgekeurd is, vereist altijd een nieuwe keuring en kost dus tijd.
- Het Besluit vereist, en daardoor ook de Keuringsdienst, dat een technisch hulpmiddel aan alle eisen dient te voldoen, wil het technisch hulpmiddel goedgekeurd worden. De opsporingspraktijk stelt echter vragen over het nut en de noodzakelijkheid van (het voldoen aan) alle eisen.
- De inzet van technische hulpmiddelen gebeurt in een omgeving die Digit, het politieteam dat de bevoegdheid uitvoert, niet altijd onder controle heeft. Digit heeft bijvoorbeeld géén invloed op wat een verdachte met zijn of haar geautomatiseerd werk doet. Handelingen van de eigenaar van het geautomatiseerd werk kunnen de kwaliteit van de verzamelde gegevens aantasten. Digit zou zich meer willen richten op het maken van een risicoanalyse met betrekking tot het gebruikte technisch hulpmiddel en op de bewijswaarde van de verzamelde gegevens.
- Bij een risicoanalyse gaat het om de vraag hoe groot het risico is dat de kwaliteit van gegevens in het gedrang komt als een technisch hulpmiddel wordt gebruikt dat niet aan alle eisen voldoet.
- Het is verder de vraag wat het gebruik van een technisch hulpmiddel, dat niet aan alle eisen voldoet, betekent voor de bewijswaarde van de verzamelde gegevens. Zeker wanneer de gegevens slechts een deel vormen van het bewijs dat verzameld is.

In de opsporingsonderzoeken waarin de hackbevoegdheid is ingezet werd in de meerderheid van de onderzoeken gebruikgemaakt van een commercieel product. Ook hiervoor geldt dat geen gebruik is gemaakt van een vooraf goedgekeurd hulpmiddel. Sterker nog, het product is nooit ter keuring aangeboden, omdat de Digit-officier, de landelijk officier die de bevoegdheid in portefeuille heeft, oordeelde dat de aard van dit hulpmiddel zich verzet tegen een keuring. Daarbij maakte de officier van justitie gebruik van een uitzonderingsgrond in het Besluit. Dit product kan overigens onder het huidige keuringsregime ook niet goedgekeurd worden. Een aantal punten maakt dat een commercieel product naar zijn aard niet te keuren is en/of nooit goedgekeurd zal worden (Van Uden & Van den Eeden, 2022, p. 134-147):

- Commerciële middelen worden relatief vaak geüpdatet. De vraag is welke versie(s) de Keuringsdienst moet keuren. Mocht dit bij alle versies noodzakelijk zijn, dan past dat niet bij de doorlooptijd die een keuring doorgaans in beslag neemt in relatie tot de termijn waarbinnen een inzet plaats moet vinden.

- De exacte werking van dit soort middelen is voor de gebruikers ervan een 'zwarte doos'. Daardoor krijgt de Keuringsdienst geen inzage in de precieze werking en kan geen volledige keuring plaatsvinden.
- Een leverancier heeft te allen tijde toegang tot zijn product, bijvoorbeeld voor het plegen van onderhoud. Daardoor krijgt de Keuringsdienst geen exclusieve toegang tot het middel, hetgeen voor haar een vereiste is om de keuring te kunnen doen. Geen exclusieve toegang betekent geen goedkeuring, omdat niet uitgesloten kan worden dat een andere partij dan de verdachte en de politie toegang heeft gehad tot de verzamelde gegevens. Dat betekent dat de betrouwbaarheid en de integriteit van de gegevens niet volledig gegarandeerd kunnen worden.

Het niet uitvoeren van een keuring leidt ertoe dat in een meerderheid van de opsporingsonderzoeken niet voldaan wordt aan een belangrijke waarborg ten aanzien van de kwaliteit van de verzamelde gegevens. Daarbij dient opgemerkt te worden dat in deze situatie wel aanvullende technische en tactische waarborgen worden getroffen om de betrouwbaarheid van het bewijs te kunnen garanderen. Deze tactische waarborgen worden tijdens de keuring niet meegenomen.

8.2 Algemene observaties buitenland

Uit onze algemene inventarisatie komt naar voren dat de nadruk van het wettelijk kader in het buitenland ligt op de rechtmatigheid van de hackbevoegdheid. Het merendeel van de waarborgen heeft betrekking op de proportionaliteit van de bevoegdheid. Hierbij gaat het onder meer om:

- het type misdrijf waarvoor de bevoegdheid mag worden ingezet;
- de doelbinding van de bevoegdheid: wordt de bevoegdheid gebruikt voor de wettelijke doeleinden waarvoor hij mag worden ingezet?;
- de onderzoekshandelingen die mogen worden uitgevoerd met de bevoegdheid;
- de termijn van de inzet van de bevoegdheid;
- de impact die de inzet van de bevoegdheid heeft op het geautomatiseerd werk van de verdachte: in hoeverre tast de inzet van het technisch hulpmiddel de werking of de beveiliging van het geautomatiseerd werk (blijvend) aan.

Dit wil overigens niet zeggen dat er in deze landen verder geen aanvullende waarborgen aanwezig kunnen zijn. Het is bijvoorbeeld mogelijk dat de politie interne beleidsregels hanteert. Deze zijn voor zover ons bekend niet publiekelijk beschikbaar, waardoor formeel onbekend is wat die precieze regels zijn. Wel is in ons onderzoek duidelijk geworden dat in veel landen tekst en uitleg moet worden gegeven over de werkzaamheden die zijn verricht door de politie, mocht een zittingsrechter de zaak behandelen. Hoewel wij dus geen volledig inzicht hebben kunnen krijgen in (de inhoud van) de aanwezige beleidsregels binnen de politie in de verschillende landen, lijkt het op basis van de inventarisatie aannemelijk te zijn dat de politie bepaalde *best practices* zal hanteren om de legitimiteit en bewijswaarde van de verkregen gegevens aan te tonen.

Tijdens ons onderzoek is vrijwel geen jurisprudentie naar voren gekomen waarin de kwaliteit van de daarmee verzamelde gegevens bediscussieerd is. Dit schept helaas geen verdere duidelijkheid over de *best practices* die al dan niet worden gehanteerd en hoe een zittingsrechter deze waardeert. Dat er geen jurisprudentie naar voren is gekomen, wil overigens niet zeggen dat de kwaliteit van de gegevens niet ter discussie

is gesteld, maar slechts dat dit niet in de uitspraak terecht is gekomen. Geïnterviewden geven op basis van eigen ervaring aan weinig zaken te kennen waarin de kwaliteit van de gegevens ter discussie wordt gesteld. Zij verwachten dat dit in de toekomst meer zal gebeuren. Dat dit nu nog niet gebeurd is, zou volgens geïnterviewden onder meer kunnen komen doordat de bevoegdheid relatief nieuw is, door een gebrek aan technische kennis bij de verdediging en/of het aanvullende (overtuigend) bewijs dat gepresenteerd wordt.

8.3 Landenvergelijking

In ons onderzoek zijn vijf landen meer diepgaand bestudeerd: België, Duitsland, Frankrijk, Zweden en Zwitserland. In de onderliggende subparagrafen worden deze landen onderling vergeleken en wordt een vergelijking gemaakt met Nederland. Dat gebeurt met betrekking tot de waarborgen voorafgaand aan de inzet, tijdens de inzet en na de inzet van de hackbevoegdheid. De aandacht wordt gericht op de meest opvallende punten.[250]

8.3.1 Waarborgen voorafgaand aan inzet bevoegdheid

Tabel 8.1 geeft een overzicht van de waarborgen die gelden voorafgaand aan de inzet van de bevoegdheid (voordat een geautomatiseerd werk gehackt wordt).

Tabel 8.1 Overzicht waarborgen voorafgaand aan inzet bevoegdheid

Land	Waarborg
België	Politie test technisch hulpmiddel zelf op basis van interne (vertrouwelijke) regels.
Duitsland	Een technisch hulpmiddel moet zo worden ingesteld dat het alleen lopende communicatie of de inhoud en de omstandigheden van de communicatie opneemt.
	Er mogen alleen wijzigingen op het geautomatiseerd werk worden aangebracht die strikt noodzakelijk zijn.
	Er zijn eisen geformuleerd waaraan leveranciers dienen te voldoen. De gebruiker van de software of een daartoe aangewezen instantie toetst deze. De SLB-richtlijn dient daarbij als leidraad voor de toets. Onderdeel daarvan is een risicoanalyse van het technisch hulpmiddel en de omgeving.
	Overheidsorganisatie ZITiS kan helpen bij de aanschaf van technische hulpmiddelen en bij het toetsen of deze middelen binnen het wettelijker kader passen. Dit is echter geen formele keuring. In de toekomst is het plan dat zij zelf ook technische hulpmiddelen gaat ontwikkelen.
Frankrijk	De overheidsdienst STNCJ is verantwoordelijk voor de aanschaf van technische hulpmiddelen en voor de uitvoering van de hackbevoegdheid. Het is onbekend welke criteria zij hanteert voor de aanschaf en het beoordelen van de middelen.

[250] Zoals eerder opgemerkt is het onduidelijk of en hoe interne beleidsregels van de politie eruitzien. Het is daarom mogelijk dat landen meer waarborgen kennen dan in de komende paragrafen besproken worden.

Land	Waarborg
Nederland	Voorafgaand aan een inzet keurt de Keuringsdienst een technisch hulpmiddel aan de hand van een keuringsprotocol. Dit protocol is gebaseerd op diverse artikelen uit het Besluit.
	In beginsel kan een technisch hulpmiddel alleen worden ingezet als deze vooraf is goedgekeurd door de Keuringsdienst. Hiervoor geldt een aantal uitzonderingen: keuring achteraf, een handmatige inzet en het middel is 'naar zijn aard' niet te keuren.
Zweden	Functionaliteiten van een technisch hulpmiddel worden beperkt in lijn met de inhoud van het bevel.
	Een technisch hulpmiddel mag geen onnodige schade veroorzaken.
	Gestandaardiseerde software en tools van andere politiediensten kunnen worden gebruikt.
Zwitserland	Functionaliteiten van het technisch hulpmiddel dienen te worden beperkt (alleen interceptie van communicatie).
	Er is een beperkte toegang tot de gegevens: een leverancier van GovWare mag geen toegang hebben tot gegevens.
	De politie test het technisch hulpmiddel zelf op basis van interne (vertrouwelijke) regels.

Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. De wijze waarop verschilt echter per land. Nederland kent de meest gedetailleerde *beschreven* keuring van technische hulpmiddelen. De wijze waarop Duitsland de criteria heeft beschreven lijkt het meest in de buurt te komen bij de wijze waarop Nederland dat heeft gedaan. De Duitse keuring is gebaseerd op de SLB-richtlijn,[251] waarbij de volgende thema's centraal staan: beschermingsdoelen en veiligheidsmaatregelen, werkprocessen en procedures, leveranciers en testbeleid. Het hanteren van de richtlijn is geen wettelijk vereiste, maar geldt als leidraad. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten (denk aan systeemcomponenten zoals hard- en software, applicaties, organisatorische of personele aangelegenheden) risico lopen. De resultaten van die risicoanalyse, de vaststelling van de beschermingsbehoeften en de daaruit voortvloeiende gevolgen en de uitvoering ervan, worden vastgelegd in een IT-beveiligingsconcept. Zowel leveranciers van software als gebruikers van de software dienen zich aan dit concept te conformeren. In de overige landen hebben we niet kunnen achterhalen welke criteria deel uitmaken van de keuring.

In Nederland wordt de keuring uitgevoerd door de Keuringsdienst. De Keuringsdienst is onafhankelijk, maar valt formeel onder hetzelfde organisatieonderdeel van de Nationale Politie als waar het team toebehoort dat de bevoegdheid uitvoert. In Frankrijk voert een specifieke overheidsinstantie genaamd STNCJ de keuring uit. Deze instantie is ook verantwoordelijk voor de uitvoering van de bevoegdheid. In beide landen kan door de wijze waarop de taken zijn belegd de vraag rijzen hoe onafhankelijk de keuring is. Dit geldt in het bijzonder voor Frankrijk, waarbij het ook daadwerkelijk dezelfde organisatie is die uitvoert en keurt. In de andere landen toetst de politie zelf. Ook in Zwitserland is de 'keurder' (zij hebben geen formele keuring,

[251] Voluit '*Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung*'.

maar testen de middelen wel) en uitvoerder dezelfde partij. In Zwitserland en Frankrijk wordt deze dubbelrol niet als problematisch gezien en wordt aangenomen dat de partijen in principe vertrouwenswaardig handelen. In Zweden vindt – voor zover bekend – geen formele keuring plaats. Wel wordt daar later in het proces van het hacken – als de gegevens op de systemen van de politie staan – veelal gebruik-gemaakt van gestandaardiseerde software. Dit is bijvoorbeeld software gecertificeerd door andere politiediensten, zoals de Nederlandse politie.

8.3.2 Waarborgen tijdens inzet bevoegdheid

Tabel 8.2 geeft een overzicht van de waarborgen die gelden tijdens de inzet van de bevoegdheid (de periode dat er toegang is tot een geautomatiseerd werk en gegevens worden binnengehaald).

Tabel 8.2 Overzicht waarborgen tijdens inzet bevoegdheid

Land	Waarborg
België	Om de vijf dagen brengt de politie schriftelijk verslag uit aan een onderzoeksrechter. De onderzoeksrechter kan besluiten de inzet te beëindigen.
Duitsland	Technische hulpmiddelen dienen, volgens de stand van de techniek, bescherming te bieden tegen ongeoorloofd gebruik door derden.
	In de SLB-richtlijn zijn criteria vastgelegd met betrekking tot de technische hulpmiddelen die gebruikt gaan worden.
	Gekopieerde gegevens moeten, volgens de stand van de techniek, worden beschermd tegen wijziging, ongeoorloofde verwijdering en ongeoorloofde toegang door derden.
	Updates van technische hulpmiddelen dienen direct doorgevoerd te worden.
	Logging en documentatie van de gegevensverzameling moeten plaatsvinden.
	In de verslaglegging dient aandacht besteed te worden aan de volgende onderwerpen: benaming en tijdstip, identificatie van het geautomatiseerd werk en aangebrachte wijzigingen, informatie aan de hand waarvan gegevens kunnen worden vastgelegd en de eenheid die de bevoegdheid uitvoert.
Frankrijk	De uitvoering van de bevoegdheid vindt plaats onder toezicht van de magistraat die toestemming verleent.
	STNCJ is verantwoordelijk voor de opslag van de verkregen gegevens.
Nederland	Gedurende de inzet moeten alle onderzoekshandelingen worden gelogd.
	Het transport van gegevens van het geautomatiseerd werk naar de technische infrastructuur van de politie dient op een veilige (versleutelde) manier plaats te vinden.
	Opslag van de verkregen gegevens vindt plaats op een beveiligde infrastructuur van de politie.
	Gedurende de inzet kan toezicht plaatsvinden door de Inspectie.
	In de verslaglegging dient het volgende te worden opgenomen: eventuele onregelmatigheden, plaatsing van het technisch hulpmiddel, verrichtte onderzoekshandelingen, (niet volledige) verwijdering van een technisch

Land	Waarborg
	hulpmiddel en selectie van gegevens indien bewerkingen hebben plaatsgevonden.
Zweden	Interne beleidsregels (niet openbaar).
Zwitserland	Het vastleggen van gegevens moet onveranderlijk en zonder onderbreking plaatsvinden.
	Het transporteren van gegevens tussen het geautomatiseerd werk en de systemen van de politie moet veilig verlopen.
	De politie dient een verslag te schrijven over de handelingen die zijn verricht.

De waarborgen tijdens de inzet van de bevoegdheid verschillen per land. Gangbare waarborgen in deze fase zijn vormen van logging, verslaglegging, het gebruik van een beveiligd transport van gegevens afkomstig uit het geautomatiseerd werk en het opslaan van de gegevens in een beveiligde omgeving. Hoewel bij Zweden in deze tabel geen waarborgen staan, is bekend dat de Zweedse politie interne beleidsregels hanteert waarin verschillende waarborgen zijn opgenomen. Deze beleidsregels zijn echter niet openbaar beschikbaar.

In België en Frankrijk vindt gedurende de inzet van de bevoegdheid rechterlijk toezicht plaats. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de bevoegdheid. Indien de uitvoering van de bevoegdheid niet conform de voorwaarden van de toestemming plaatsvindt, kan de inzet van de bevoegdheid worden stopgezet. Daarbij moet worden opgemerkt dat de rechter afhankelijk is van de informatie die de politie of de officier van justitie tussentijds verstrekt of kan verstrekken. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk voor zal zorgen dat een inzet tussentijds beëindigd zal worden. Het rechterlijk toezicht in deze landen gaat verder dan de rol van de rechter-commissaris in Nederland, die in principe alleen voorafgaand aan een inzet (of een verlenging ervan) meekijkt. Wel kent Nederland nog het toezicht door de Inspectie Justitie en Veiligheid.

8.3.3 Waarborgen na inzet bevoegdheid

Tabel 8.3 geeft een overzicht van de verschillende waarborgen wat betreft de periode nadat de inzet van de bevoegdheid heeft plaatsgevonden (het moment dat de politie geen toegang meer heeft/mag hebben tot het geautomatiseerd werk en er geen gegevens meer verzameld worden).

Tabel 8.3 Overzicht waarborgen na inzet bevoegdheid

Land	Waarborg
België	Notificatie over de aard en de looptijd van de inzet dient plaats te vinden. Notificatie kan in principe niet achterwege worden gelaten, tenzij de identiteit of de woonplaats van de verdachte redelijkerwijs niet achterhaald kan worden.
	De onderzoeksrechter bepaalt welke informatie van belang is voor het dossier. Alle gebruikte stukken die niet aan het dossier worden toegevoegd, worden òf vernietigd òf (verzegeld) naar de griffie gestuurd. De verdediging kan de onderzoeksrechter verzoeken informatie toe te voegen aan het dossier.
Duitsland	De aangebrachte wijzigingen aan het geautomatiseerd werk moeten, indien technisch mogelijk, na beëindiging van de inzet van de bevoegdheid automatisch ongedaan gemaakt worden.
	Notificatie dat de bevoegdheid is ingezet dient plaats te vinden. Notificatie kan onder voorwaarden worden uitgesteld en uiteindelijk afgesteld.
	De gebruikte software moet gearchiveerd worden.
	De verdediging kan de kwaliteit van de software ter discussie stellen aan de hand van de gegevens die zij tot haar beschikking krijgt.
Frankrijk	Een betrokkene wordt alleen genotificeerd als een zaak ter zitting komt. Er geldt géén notificatieplicht.
	Op zitting wordt een transcript van de gegevens verstrekt maar verder wordt geen informatie gegeven over waar deze gegevens vandaan komen en hoe deze zijn verkregen. In bijzondere gevallen kan de advocaat vragen informatie te declassificeren. Indien een zittingsrechter aan dat verzoek gehoor geeft, kan meer informatie worden verstrekt.
Nederland	Een betrokkene dient te worden genotificeerd nadat de inzet van de bevoegdheid heeft plaatsgevonden. Uitstel van notificatie is mogelijk.
	De Inspectie Justitie en Veiligheid kan zowel tijdens als achteraf toezicht houden op de uitvoering van de bevoegdheid.
	Na beëindiging van een inzet, wordt het technisch hulpmiddel voor zover als mogelijk verwijderd.
	De verdachte krijgt inzage in de gegevens die als bewijsmateriaal zijn opgenomen in het dossier. De verdediging kan gemotiveerd vragen om extra gegevens in te zien.
Zweden	Bij notificatie dient de volgende informatie te worden gegeven: welke bevoegdheid is ingezet, de looptijd van de inzet, welke geautomatiseerde werken zijn binnengedrongen en op welke locaties. In het geval van specifieke misdrijven kan notificatie achterwege blijven, indien opsporingsbelangen geschaad worden.
	Alle verzamelde gegevens zijn gemotiveerd opvraagbaar voor de verdediging. Beide partijen kunnen een extern expert raadplegen.
	Tijdens de zitting wordt geen informatie prijsgegeven over de werking van het technisch hulpmiddel.

Land	Waarborg
	Een technisch hulpmiddel moet verwijderd worden en de beveiliging van het geautomatiseerd werkt moet op zijn minst hetzelfde niveau hebben als vóór de inzet.
	De Commissie voor Veiligheid en Integriteitsbescherming (SIN) houdt toezicht op de inzet van de bevoegdheid (in principe achteraf).
Zwitserland	In de notificatie dient aandacht te worden besteed aan: reden, aard en looptijd van de inzet. Met toestemming van de Dwangmiddelenrechtbank kan notificatie achterwege blijven.
	De verdachte kan inzage krijgen in de opnames.
	De broncode van het technisch hulpmiddel moet gecontroleerd kunnen worden als de rechtbank daar om vraagt.
	Het technisch hulpmiddel moet na de inzet gedeactiveerd worden.

De meest voorkomende waarborgen hebben betrekking op de notificatie van de inzet van de bevoegdheid aan de verdachte(-n) of betrokkene(-n), de inhoudelijke behandeling tijdens de zitting en het inzagerecht van de verdachte. Notificatie is niet in alle landen gegarandeerd, omdat dit soms achterwege kan blijven indien het risico bestaat dat lopende opsporingsbelangen worden geschaad. In België moet op basis van de wet altijd genotificeerd worden. Frankrijk is het enige land waarin een verdachte niet genotificeerd hoeft te worden. Uiteraard geldt dat, indien de gehackte gegevens deel uitmaken van de bewijsvoering, de verdachte door inzage in het dossier indirect wordt genotificeerd. Welke informatie in het dossier wordt opgenomen, en tot hoever het inzagerecht strekt, is niet voor alle landen duidelijk geworden. Wel komt naar voren dat in de meeste gevallen de verdediging een kopie ontvangt van (een selectie van) de gegevens die verzameld zijn met de hackbevoegdheid.

Op basis van de interviews blijkt dat nog weinig jurisprudentie beschikbaar is waarin de kwaliteit van de gegevens, verzameld met behulp van de hackbevoegdheid, ter discussie is gesteld. Dat maakt het lastig om de vraag te beantwoorden in welke mate een zittingsrechter de inzet van de bevoegdheid en de kwaliteit van de gegevens toetst. De jurisprudentie die ons wel bekend is gaat veelal over zaken waarin bewijs wordt gebruikt gebaseerd op gegevens van de communicatiedienst Encrochat. De Franse autoriteiten hebben deze communicatie kunnen onderscheppen. In veel landen zijn Encrochat-gegevens gebruikt als bewijs. Bij de behandeling van deze zaken stond echter vooral de vraag centraal of het verkregen bewijs rechtmatig was en niet de vraag wat de kwaliteit van de verzamelde gegevens was. Voor zover bekend is alleen in Zweden en Frankrijk de kwaliteit van gegevens ter discussie gesteld. In Zweden verwierp de rechtbank relatief eenvoudig de geuite bezwaren ten aanzien van de kwaliteit van de gegevens. Zij concludeerde dat de gepresenteerde gegevens in samenhang met andere opsporingsgegevens laten zien dat 'de berichten qua tijd en inhoud goed overeenkomen met de werkelijkheid'.[252] Opvallender is een arrest van oktober 2022 uit Frankrijk.[253] Daarin concludeert de rechter dat, bij gebrek aan een certificaat van waarheidsgetrouwheid, het niet wordt geaccepteerd dat niets gedeeld wordt over de wijze waarop het bewijs verkregen is. Dit geldt echter alleen als de verzamelde gegevens versleuteld zijn. Het ligt voor de hand dat de politie de

[252] Uitspraak rechtbank Stockholm d.d. 22 april 2021 in zaak nr. B 5546-20, p. 9.
[253] Hof van Cassatie, strafkamer, 11 oktober 2022, beroep nr. 21-85.148.

bevoegdheid juist inzet om ontsleutelde berichten (live) te kunnen inzien. In deze gevallen is een certificaat dus niet benodigd.

Een ander opvallend punt ten aanzien van de waarborgen na afloop van de inzet is de wettelijke bepaling in Zwitserland dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Voorafgaand aan de inzet moet ook worden verzekerd dat de leverancier geen toegang kan krijgen tot de gegevens. Het prijsgeven van de broncode en de toegangsbeperking vallen op, omdat beide punten in Nederland een belangrijk obstakel vormen om commerciële middelen te keuren en goed te keuren. Een relevante vraag, die helaas niet beantwoord kan worden op basis van ons onderzoek, is daarom in hoeverre beide vereisten uiteindelijk afgedwongen kunnen worden in Zwitserland.

Ten slotte valt op dat Zweden het enige van de vijf landen is dat een specifieke toezichthouder (SIN) kent die toezicht houdt op de bevoegdheid. De rol van SIN ten aanzien van de inzet van technische hulpmiddelen voor de hackbevoegdheid is nog in ontwikkeling. Het toezicht richt zich vooralsnog vooral op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid). SIN heeft echter de bevoegdheid om ook naar de technische hulpmiddelen zelf te kijken. De uitspraken van SIN zijn niet bindend, maar over het algemeen volgen instanties de uitspraken wel op. SIN heeft deels vergelijkbare taken als de Inspectie in Nederland, maar houdt daarnaast toezicht op de rechtmatigheid van het hele proces en daarmee ook de activiteiten van zowel de politie als het Openbaar Ministerie. Verder kan SIN publiekelijk uitspraken doen in individuele zaken. De verdachte kan hier ook persoonlijk om vragen.

Het voorgaande heeft laten zien dat Nederland ten opzichte van de andere landen een erg gedetailleerd keuringsproces heeft vastgelegd. Uit onze inventarisatie komt naar voren dat vier van de vijf landen technische hulpmiddelen toetsen alvorens ze worden aangeschaft en ingezet. Het is echter onduidelijk hoe vergaand deze toets is en in hoeverre de kwaliteit van gegevens in deze toets een belangrijke rol speelt. Verder ligt het zwaartepunt van de waarborgen in deze landen in de laatste fase van de inzet van de bevoegdheid. Na de inzet van de bevoegdheid kan de kwaliteit van gegevens tijdens de zitting ter discussie worden gesteld. In Nederland moet de keuring in principe zorgen dat de kwaliteit van de verkregen gegevens niet ter discussie wordt gesteld.

8.4 Slotbeschouwing

Op basis van ons onderzoek hebben wij een drietal scenario's geformuleerd die mogelijk een aanvulling kunnen bieden op de wijze waarop in Nederland met technische hulpmiddelen en gegevens, verzameld middels de hackbevoegdheid, wordt omgegaan. Deze scenario's worden in onderstaande tekst beschreven.

Scenario 1: Broncode en controle op toegang gegevens
In ons onderzoek komt naar voren dat het in Zwitserland wettelijk verplicht is dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Daarnaast moet verzekerd worden dat de leverancier geen toegang kan krijgen tot de gegevens wanneer deze verzameld worden. Juist deze twee punten vormen een belangrijk obstakel in Nederland om commerciële technische hulpmiddelen te keuren. Het is niet duidelijk geworden in hoeverre de Zwitserse

autoriteiten daadwerkelijk beide vereisten hebben kunnen realiseren. Voor zover bekend is er nog geen zaak geweest waarin daadwerkelijk om de broncode is gevraagd. De leverancier heeft er in beginsel geen baat bij om inzage te geven in zijn broncode. De werkwijze van de software is een goed bewaard geheim. Echter, als Zwitserland een werkbare oplossing heeft kunnen vinden, is het voor de politie, het Openbaar Ministerie en beleidsmakers in Nederland waardevol om te verkennen hoe dit op een soortgelijke manier gerealiseerd kan worden. Daarmee zouden twee belangrijke knelpunten bij de keuring in Nederland opgeheven kunnen worden.

Scenario 2: Veranderende rol toezicht

Gedurende het Nederlandse wetstraject is het toezicht tijdens de inzet van de bevoegdheid een belangrijk discussiepunt geweest. Extra toezicht zou nodig zijn omdat rechters niet altijd in staat zouden zijn om het verzamelde bewijs goed te beoordelen. Ook was de verwachting dat een (groot) deel van de zaken nooit door een zittingsrechter behandeld zou worden. Er is geopperd om een vergelijkbaar orgaan in het leven te roepen als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Verschillende auteurs (Hildebrandt, 2016; Buruma, 2016; Schermer, 2017) pleitten in voorgaande jaren ervoor dat dit orgaan 'ook nadrukkelijk de rechtmatigheid van de gegevensverwerkingen door de politie onder leiding van het Openbaar Ministerie in het opsporingsproces toetst' (Oerlemans, 2018, p. 18-19). Fedorova en collega's (2022) komen in hun rapport tot een soortgelijke conclusie. Hirsch Ballin & Oerlemans (2022) stellen dat het huidige toezichtstelsel voor datagedreven opsporing te kort schiet en opperen eveneens een dergelijke toezichthouder op te richten. Het doel van deze toezichthouder zou zijn om als toezichthouder in de zin van de Richtlijn gegevensbescherming opsporing en vervolging te dienen en daarnaast in bredere zin een controlerende taak te hebben ten aanzien van datagedreven opsporing waar de strafrechter die rol niet kan vervullen (Hirsch Ballin en Oerlemans, 2023, p. 12). Ook de 'Commissie modernisering opsporingsonderzoek in het digitale Tijdperk' (voorts aangeduid als Commissie Koops) richt zich in haar rapport op toezicht. Zij geeft in haar aanbevelingen aan 'specifiek aandacht te besteden aan de houdbaarheid van het systeem van toezicht op de langere termijn, alsmede aan de inrichting van extern toezicht op de gegevensvergaring en -verwerking door opsporingsdiensten' (Commissie Koops, 2018, p. 31). De commissie noemde echter geen specifieke maatregelen, zoals het instellen van een aparte commissie naar voorbeeld van de CTIVD. Voor de instelling van zo'n commissie is uiteindelijk niet gekozen (Van Uden & Van den Eeden, 2022, p. 206-207). Argumenten hiervoor waren het reeds bestaande toezicht door een rechter-commissaris en het toezicht door de Centrale Toetsingscommissie van het Openbaar Ministerie (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 20). In plaats daarvan is gekozen voor de Inspectie Justitie en Veiligheid, die toezicht houdt op zaken die wel en niet aan de rechter worden voorgelegd (Van Uden & Van den Eeden, 2022, p. 207).

Op basis van ons onderzoek nemen wij geen positie in ten aanzien van deze discussie. Wel is het relevant om te noemen dat, als ten aanzien van de hackbevoegdheid de rol van het toezicht verder wordt verkend, een aantal landen in onderhavig onderzoek naar voren is gekomen dat mogelijk handvatten kan bieden.

Ten eerste is in dit kader relevant dat in België en Frankrijk een onderzoeksrechter toezicht houdt op de uitvoering van de bevoegdheid. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de bevoegdheid. Indien nodig kan de rechter besluiten de inzet van de bevoegdheid stop te zetten. Dit toezicht gaat verder dan de rol van de rechter-commissaris, die in

principe alleen voorafgaand aan een inzet controle uitoefent. De werkwijze in België en Frankrijk ondervangt het probleem dat een deel van de zaken niet door de zittingsrechter wordt behandeld. Als kanttekening moet worden opgemerkt dat de rechter afhankelijk is van de informatie die hij of zij verstrekt krijgt. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk toe leidt dat gedurende een inzet een inhoudelijke toets plaatsvindt. Wel biedt het een perspectief dat afwijkt van de Nederlandse systematiek, waarin de rechter-commissaris voorafgaand toestemming verleent en daarna in principe niet meer toeziet op de uitvoering van de bevoegdheid.
Ten tweede is de Zweedse toezichthouder (SIN) relevant. Deze toezichthouder houdt specifiek toezicht op de uitvoering van de hackbevoegdheid. Hij lijkt daarmee op de – door sommige auteurs voorgestelde – commissie naar voorbeeld van de CTIVD. SIN richt zich vooralsnog primair op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid) en houdt zowel toezicht op de activiteiten van de politie als van het Openbaar Ministerie. Hiermee onderscheidt hij zich van de taken van de Inspectie in Nederland die alleen toezicht houdt op de politie. Daarnaast kan SIN op verzoek en uit eigen beweging publiekelijk uitspraken doen in individuele zaken. Doordat SIN zich zowel richt op de juridische als op de procesmatige aspecten worden de eerder aangehaalde problemen ondervangen dat niet alle zaken voor een zittingsrechter komen en dat de rechter niet altijd voldoende in staat zou zijn al het bewijs goed te beoordelen.

Scenario 3: Keuring op maat
Zoals reeds besproken vormt de keuring in Nederland een belangrijke waarborg bij de inzet van technische hulpmiddelen en de kwaliteit van de gegevens die met het middel worden verzameld. In de praktijk blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk is bedoeld. Er wordt voornamelijk gebruikgemaakt van niet vooraf goedgekeurde technische hulpmiddelen en technische hulpmiddelen die naar hun aard niet te keuren zijn. Opvallend is dat in het buitenland de waarborgen rondom technische hulpmiddelen en de kwaliteit van gegevens wettelijk minder gedetailleerd beschreven zijn dan in Nederland. In dat opzicht is het in het buitenland gemakkelijker om de bevoegdheid in te zetten. Ook valt op dat in die landen (vooralsnog en voor zover ons bekend) niet of nauwelijks jurisprudentie beschikbaar is die het gebruik van de hackbevoegdheid in deze landen ter discussie stelt. Dat betekent overigens niet dat het bewijs van de hackbevoegdheid altijd zomaar geaccepteerd zal worden. In veel landen is de hackbevoegdheid relatief nieuw en zal het gebruik ervan en een oordeel daarover zich nog verder ontwikkelen. Het valt dan ook niet uit te sluiten dat in de toekomst alsnog uitspraken volgen die gevolgen hebben voor het huidig wettelijke kader in deze landen. Dat neemt niet weg dat het interessant is om te constateren dat in de verschillende landen niet de keuze is gemaakt om de kwaliteit van de gegevens te controleren op een wijze waarop Nederland dat doet. En dat de buitenlandse manier van werken voor zover bekend vooralsnog niet tot wezenlijke discussies in de rechtbank heeft geleid. Daarom hebben we een derde scenario opgenomen waarin oog is voor meer maatwerk ten aanzien van de keuringseisen, waarbij aandacht is voor aanvullende tactische en technische waarborgen. Dit scenario verkent (a) het gebruik van een risicoanalyse in de keuring en (b) de vraag in hoeverre aanvullende tactische en technische maatregelen voldoende gewaarborgd zijn.

Scenario 3a: Risicoanalyse in de keuring
In Duitsland speelt het maken van risicoanalyses een rol wanneer het gaat om de aanschaf en het gebruik van technische hulpmiddelen. In een SLB-richtlijn worden diverse onderwerpen genoemd waarmee rekening zou moeten worden gehouden als

het gaat om technische hulpmiddelen, zoals het testbeleid. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten risico lopen en welke aanvullende maatregelen nodig zijn. De verschillende betrokken partijen dienen zich hieraan te conformeren. In Nederland geeft de uitvoerende partij (Digit) aan dat de Keuringsdienst (en het onderliggende keuringsprotocol) onvoldoende rekening houdt met het feit dat zij ook zou kunnen werken op basis van risicoanalyses, namelijk wat betreft de maatregelen die zij neemt wanneer zij een inzet doet met een technisch hulpmiddel. Juist deze risicoanalyse lijkt een meer centrale plek te hebben in Duitsland. Daarom zou de werkwijze in Duitsland nader verkend kunnen worden om te zien wat daaruit geleerd kan worden voor de Nederlandse situatie.

Scenario 3b: Borging aanvullende tactische waarborgen in Nederland
Zoals opgemerkt, wordt in Nederland op dit moment primair gebruikgemaakt van technische hulpmiddelen waarvan de officier van justitie oordeelt dat ze naar hun aard niet te keuren zijn. In deze situatie worden tactische en technische maatregelen getroffen om de kwaliteit van de gegevens te waarborgen. Voor nu zijn er geen aanwijzingen dat het gebruik van commerciële producten beëindigd zal worden. De huidige minister ziet deze als 'een realiteit waar we mee te dealen hebben', zo blijkt uit een Commissiedebat op 7 juli 2022.[254] Het gebruik van risicoanalyses beschreven in scenario 3a kan een handvat bieden om juiste aanvullende maatregelen te treffen om de kwaliteit van gegevens te waarborgen. Indien de werkwijze met commerciële producten eerder regel dan uitzondering blijft en exact op dezelfde manier gewerkt zal blijven worden, is het ook van belang de rol van het Openbaar Ministerie ten aanzien van de aanvullende (tactische) waarborgen tegen het licht te houden. Op dit moment is zij de enige die voorafgaand aan een inzet deze waarborgen bekijkt. Een tactisch officier van justitie die het opsporingsonderzoek leidt is in principe eindverantwoordelijk voor de tactische waarborgen. Deze worden ook bekeken door de Digit officier van justitie en de Centrale toetsingscommissie van het Openbaar Ministerie. Vanwege enkel de betrokkenheid van het Openbaar Ministerie en geen andere onafhankelijke instantie, is het nuttig om te verkennen welke andere partij (aanvullend) kan controleren of deze maatregelen toereikend zijn, zeker in gevallen dat een zittingsrechter een zaak niet zal behandelen.

Tot besluit
Voor veel landen geldt dat de hackbevoegdheid een relatief nieuwe bevoegdheid is. Daarnaast is de daarvoor benodigde digitale expertise voor veel betrokkenen relatief nieuw. Dit leidt ertoe dat wet- en regelgeving niet altijd aansluiten op de praktijk. In Nederland zien wij dit terugkomen in de knelpunten rondom het keuringsproces. In het buitenland kunnen wij ons voorstellen dat in de toekomst wet- en regelgeving voor de kwaliteit van de gegevens worden aangescherpt. Mogelijk aangejaagd door jurisprudentie waarin de kwaliteit van gegevens ter discussie wordt gesteld. Op welke termijn dit gebeurt, is afwachten.

De huidige regelgeving levert in de Nederlandse uitvoeringspraktijk knelpunten op, zeker ten aanzien van de keuring van technische hulpmiddelen. Anders dan de wetgever had bedoeld worden niet of nauwelijks technische hulpmiddelen ingezet die voorafgaand aan de inzet ervan goedgekeurd zijn. Dit geldt zowel voor commerciële producten als eigen ontwikkelde middelen. Vanwege de aard en de meerwaarde van deze technische hulpmiddelen is het aannemelijk dat deze situatie voorlopig zal aanhouden. Om de kwaliteit van gegevens verkregen met deze hulpmiddelen te waarborgen is het zinvol om te verkennen welke aanvullende maatregelen getroffen

[254] *Kamerstukken II* 2021/22, 29 628, nr. 1122, p. 33.

kunnen worden. De door ons geschetste scenario’s kunnen hiervoor een handvat bieden.

Summary

Police Hacking regulation abroad

A comparative law study into legal regulations and safeguards regarding the quality of data

The Computer Crime Act III (CCIII) came into effect on 1 March 2019. Among other things, this Act introduces the power of the police to carry out hacking operations. The new Sections 126nba, 126uba, 126zpa in the Code of Criminal Procedure will allow specially authorised investigating officers to covertly and remotely intrude into computer systems under certain conditions and investigate them. The police can carry out investigative actions using technical tools. may be carried out with a technical aid. In principle, a technical device must be inspected and approved by an independent inspection service (*de Keuringsdienst*) prior to its use, in order to guarantee the reliability, traceability and integrity of the evidence.

The Justice & Security Inspectorate (hereinafter Inspectorate) supervises the implementation of the hacking power. In its first Report in 2020, it concluded that the use of technical tools for hacking powers and the inspection of these tools were not yet proceeding as intended under the legal framework. In his response to the first Inspectorate Report, the then Minister of Justice and Security indicated that he would have an investigation into the safeguards of technical tools used by foreign police authorities. The present report is the result of this research. This report also supplements the previously published evaluation of the use of the hacking power in the Netherlands, carried out by the WODC.

Research question

The central research question for this study is as follows:

What safeguards govern hacking powers abroad, more specifically the use of technical tools, and how does this compare with the Dutch situation?

The central research question is answered on the basis of the following subquestions:

1 What countries allow 'authorised hacking' and on the basis of which legal ground can foreign police services carry out hacking operations in their own country?
2 What statutory conditions apply in other countries for police services to deploy the hacking power?
3 To what extent do other countries test technical tools and what has been laid down in legislation and regulations on this?
4 To what extent are there any other rules to ensure the reliability, traceability and integrity of data obtained with the use of technical tools?
5 How does the working method abroad compare with the Dutch working method regarding the approval of technical tools and any other safeguards to achieve data reliability, integrity and traceability?

Methods of research

We first made a broad inventory to map out which countries have legal hacking powers. To be able to speak of a hacking power, we assumed that the hacking power is carried out secretly and remotely. As part of the broad inventory, virtually all European countries were examined, with the addition of the United States, Canada and Australia. Based on the broad inventory, a selection was made of five countries that were studied in more detail: Belgium, Germany, France, Sweden and Switzerland. Various research methods were used to answer the research questions: document study (laws and regulations and relevant (grey) literature), written questionnaires and interviews.

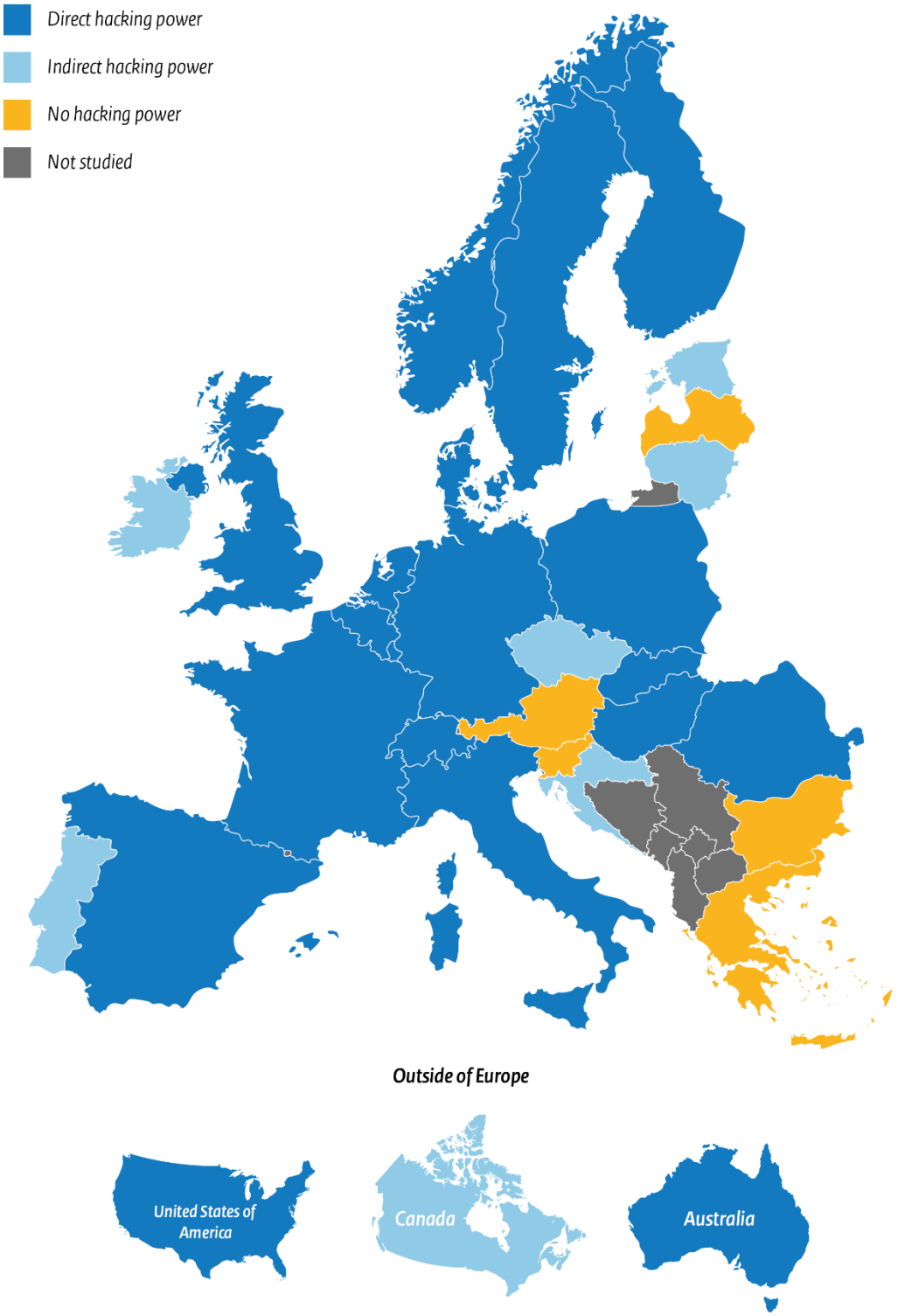
Broad inventory

Based on the broad inventory, a number of topics are discussed in this report. In this summary, attention is paid to the presence of a hacking power, the inspection of technical resources and the presence of an inspection body, the guarantees for documentation, storage and judicial supervision, and the notification obligation and the right of inspection.

Presence of hacking power

Figure S1 on the next page features a map of all the countries included in this study. The figure indicates whether a country has set up a statutory power of the police to carry out hacking operations, and if so, whether this is a direct or indirect power. A direct power applies if the law explicitly refers to the possibility of covertly and remotely intruding into a computer system and undertaking one or more investigative actions within that system. An indirect power applies if the hacking power forms part of a general provision. Consider, for example, the power to intercept telecommunications, whereby the law text does not specifically mention the hacking power, though the power could be used for that purpose.

Figure S1 Country overview – hacking power



The maps are adaptations of works by Maix (Europe; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; public domain) and Rycherr (Australia; CC BY-SA 4.0 and previous versions).

Inspection of technical tools and supervisory body

None of the countries has established an inspection by an independent inspection body in charge of testing the technical tools before they are deployed based on a comprehensive inspection protocol. Some countries do have a testing procedure, however, these procedures are not performed by an independent inspection body. Furthermore, for those other countries that do have an inspection or testing procedure, it is unknown what the procedure consists of. Germany constitutes an exception in this regard. Even in that country, it is not entirely clear what the inspection entails, but it is clear that it is based on an SLB guideline specifically designed for it. See Section 4.8.

In other countries, the supervision of hacking operations by an independent body is limited, thereby not including the trial court. Australia, Denmark, Norway, the UK and Sweden have independent bodies performing some level of supervision of the execution of the hacking power. Owing to its technical expertise, Germany has an authority that advises on the deployment and development of technical tools. France has a specific authority responsible for the design, supervision and implementation of technical tools used for hacking operations. The authorities in Sweden, Germany and France will be discussed in more detail in the coming chapters.

Safeguards regarding documentation, storage and judicial supervision

Almost all countries require some sort of documentation with regard to documenting and logging operative actions. As a minimum, they require an official report documenting all actions. Some countries take it a step further and require the logging of all actions. During our research, it remained unclear to what extent five countries have requirements to document and register operative actions.

There is judicial supervision in Belgium, France, Croatia, Portugal and Spain *during* the deployment of the hacking power. This means the police must provide interim updates on progress to the judge who issued the order. In some cases, the judge may withdraw the authorisation for the hacking operations based on those status updates. As far as we know, there is no interim judicial review in the remaining countries.

Twenty countries have included safeguards in their laws regarding the storage of data collected with the use of hacking powers. These safeguards include the sealed storage of data or the storage of data in a secure environment. In the case of the remaining countries, nothing is included in the law or it has not become clear to us whether countries have set formal or informal safeguards.

Trial and right to inspection

Thirteen countries have included a notification obligation in the law. This means that those persons whose automated information system was hacked must be informed within a predefined term that this hacking power had been deployed. In half of these countries, notification can be deferred or sometimes even omitted if the interests of the investigation may be compromised. In nearly all countries, the suspect will be notified if the case is brought before the court. Seventeen countries have explicitly included the right to inspect obtained data in legislation. In many cases, the defence

may receive a copy of the data obtained. Among the remaining countries, our inventory did not show whether this hacking power is covered by a specific legal provision regarding the right to inspection.

In-depth country comparison

A number of countries have been studied in more depth. These countries have been compared with each other and with the Netherlands. Therefore we first describe the most important bottlenecks in the Netherlands. Then follows the country comparison.

Main issues and bottlenecks in testing technical tools in the Netherlands

For the introduction of the hacking power, the Dutch legislator opted to follow the inspection system of technical tools already set in place for existing (special) investigative powers. A separate decision was prepared for the authorised hacking titled 'the Decision on intruding into computer systems (hacking)', hereinafter: the Decision. The Decision sets a number of requirements for technical tools, including requirements aimed at integrity, traceability and reliability of the data collected, hereinafter: quality. The Dutch National Commodity Inspectorate is tasked with testing the tools in the Netherlands, thereby applying an inspection protocol based on various articles from the Decision. In principle, the police must make use of technical tools that have been tested and approved prior to their use. This is subject to a number of exceptions: (1) a technical tool may be tested afterwards, (2) it is possible to switch to manual deployment or (3) the public prosecutor decides that the tool cannot be tested 'on account of its nature'.

The Reports from the and the first evaluation report from the Research and Documentation Centre show that the testing and the use of technical tools do not always proceed as intended by law. Pre-approved technical tools are hardly ever deployed, and inspection is a major bottleneck for investigation practices. Different aspects play a role here:

- The turnaround time of an inspection takes a relatively long time, at least four months. That timeframe does not always match the promptness that may be required within an investigation.
- Adjusting a technical tool that has not been approved yet always required a new inspection and thus takes time.
- The Decision demands, and consequently so does the Dutch National Commodity Inspectorate, that technical tools must meet all requirements for the technical tool to be approved. Investigation practices, however, question the usefulness and necessity of all requirements and the compliance thereof.
- The deployment of technical tools takes place in an environment which Digit, the police team executing the power, cannot always control. For example, Digit cannot exercise any influence over what suspects do with their automated information systems. Any action from the owner of the automated information system can affect the quality of the data collected. Digit would prefer to focus more on making risk analyses with regard to the technical tool used and the evidential value of the data collected.
- A risk analysis focuses on the risk of data quality being compromised if a technical tool is used that does not meet all requirements.

- Another consideration is the impact of using a technical tool that does not meet all requirements on the evidential value of the data collected. Especially, if the data only form part of the evidence collected.

The majority of police investigations in which hacking operations are carried out make use of a commercial product. Here, too, no pre-approved tools were used. In fact, the products were never submitted for testing, because the Digit public prosecutor decided that the nature of the tools preclude inspection. In so doing, the public prosecutor makes use of the Decision's ground for exception. Incidentally, these products can indeed not be approved under the current inspection regime. There are a number of factors that make a commercial tool inherently impossible to approve and/or never to be approved:

- Commercial tools are updated relatively often. The question then becomes, which version or versions should the Dutch National Commodity Inspectorate approve? If all the versions need to be approved, it would exceed the usual lead time needed for testing and approval in relation to the timeframe within which the police action must take place.
- Operation of these types of tools is a 'black box' for the users, which is why the Dutch National Commodity Inspectorate is not given access to the exact operation and can therefore not carry out a full inspection.
- Suppliers want to have access to their product at all times, to do things like perform maintenance, for example. As a result, the Dutch National Commodity Inspectorate is not given exclusive access to the tool, which it requires for its inspection. Not having exclusive access means no approval, as it cannot be ruled out that a party other than the suspect and the police had access to the data collected. This means that the reliability and integrity of the data cannot be fully guaranteed.

Failing to perform the inspection means that a majority of criminal investigations do not comply with a key safeguard with regard to the quality of the data collected. It should be noted, however, that additional technical and tactical safeguards are put in place in this situation to ensure the reliability of the evidence. These tactical safeguards are not included in the testing.

Comparison between countries

In our study, five countries have been studied in more depth: Belgium, Germany, France, Sweden and Switzerland. To compare the countries, a distinction has been made between three phases with regard to the safeguards during the deployment of the hacking power: the phase prior to deployment, during deployment and after deployment of the hacking power.

Safeguards prior to the deployment of the power

Except for Sweden, all countries have some form of inspection or testing of the technical tool to be used. However, the manner differs per country. The Netherlands has the most detailed described inspection of technical tools. The manner in which Germany has described the criteria appears closest to the way the Netherlands has done this. The German inspection is based on the SLB Guideline , which highlights the following themes: protection targets and security measures, work processes and procedures, suppliers, and test policy. Application of the guideline serves as a guiding

principle; it is not a legal requirement. A risk analysis is used to identify which objects, e.g. system components such as hardware and software, applications, organisational or personnel issues, pose a risk for these themes. The results of this risk analysis, the determination of the protection needs and the resulting consequences and implementation thereof are laid down in an IT security concept. Both software suppliers and users of the software must conform to this concept. It is not known what criteria comprise the inspections in the other countries.

The Dutch National Commodity Inspectorate carries out the inspection in the Netherlands. The Dutch National Commodity Inspectorate is an independent body, though it formally falls under the same organisational unit of the National Police Board to which the team carrying out the hacking operation belongs. In France, the testing is done by a specific government body called STNCJ. This government body is also responsible for the execution of the hacking power, which may give rise to issues of the organisation's independence. The other countries have the police doing their own testing. It is interesting to note that both in France and Switzerland, the 'inspector' and the 'performing party' are one and the same party. These countries do not consider this to be problematic and proceed on the assumption that the parties act in a fundamentally trustworthy manner. As far as known, there is no formal inspection in Sweden. However, they often use standardised software at a later stage of the hacking process, i.e. once the data are placed on the police's systems. This standardised software, for example, involves software that has been certified by other police services such as the Dutch police.

Safeguards during the deployment of the hacking power

The safeguards that must be in place during deployment of the hacking power differ per country. Common safeguards at this stage are forms of logging, reporting, the use of a secured transport of data from the automated information system and the storage of data in a secured environment. Although there are no safeguards listed in this table for Sweden, it is known that the Swedish police apply internal policy rules that include different safeguards. However, these policy rules are not publicly available.

There is judicial review in Belgium and France during the hacking operations. The judge granting authorisation for the deployment of the hacking power also supervises the execution thereof. If the execution of the hacking power does not take place in accordance with the conditions of the authorisation, the hacking operations may be terminated. It should be noted in this respect that the judge relies on the information that the police or the public prosecutor provides or may provide during the deployment. The question is thus whether this judicial oversight will actually ensure that a deployment can be terminated mid-term. The judicial oversight in these countries goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to a deployment or its extension. However, the Netherlands still has the supervision by the Inspectorate of Justice and Security.

Safeguards after the deployment of the hacking power

The most common safeguards pertain to the notification of the deployment of the hacking power to the suspects or the data subjects, the substance of the case at the hearing and the suspect's right to inspection. Notification is not a guarantee in all countries, given that such notification may be omitted if it could compromise ongoing interests of the investigation. The law in Belgium always requires notification. France is

the only country in which a suspect does not need to be notified. It goes without saying that if the data hacked form part of the evidence, the suspect is indirectly notified by the inspection of the file. Not all countries have made it clear what information is included in the file, and to what extent the right to inspection extends. However, it does emerge that in most cases the defence receives a copy of the data collected by means of hacking operations or a collection thereof.

As previously noted, there is still little case law available that calls into question the quality of the data collected by means of hacking operations. This makes it difficult to answer the question of how extensively a session judge assesses the deployment and the data quality. The case law that is available mostly deals with cases where evidence is used based on data from the Encrochat communications service. The French authorities have been able to intercept these communications. Many countries have used Encrochat data as evidence. However, the main issue in these cases was whether this was legally obtained evidence rather than the quality of the data collected. As far as known, the quality of data has only been called into question in Sweden and France. In Sweden, the court dismissed relatively easily the objections raised regarding data quality. The court added that the data, in conjunction with other investigation data, show that 'the messages correspond well to the reality in terms of time and content'. More striking is an October 2022 ruling from France. In this ruling, the court concluded that in the absence of a certificate of truthfulness, it cannot be accepted that nothing is shared about how the evidence was obtained. However, this only applies if the collected data is encrypted. It is likely that the police use the authority to view decrypted messages (live). Therefore, in these cases a certificate is not required.

Another striking issue in terms of the safeguards at the end of deployment is the legal provision applicable in Switzerland that stipulates that it must be made possible to check the source code of the technical tool if so requested by the court. Prior to deployment, it must also be ensured that the supplier cannot access the data. Source code disclosure and access restriction stand out because both issues are a major obstacle in the Netherlands to testing and approving commercial tools. A relevant question, which unfortunately cannot be answered based on our research, is thus to what extent both requirements can ultimately be enforced in Switzerland.

Finally, it is worth noting that Sweden is the only one of five countries that has a specific supervisory body (SIN) that monitors the hacking power. SIN's role in relation to the use of technical tools for the hacking power is still evolving. For the time being, supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness. However, SIN also has the authority to check the technical tools themselves. While SIN's rulings are not binding, authorities generally follow SIN's rulings. SIN has partly similar tasks to the Inspectorate in the Netherlands, but it additionally oversees the lawfulness of the entire process and thus also the activities of both the police and the public prosecutor. SIN can furthermore issue public statements in individual cases. The suspect may also personally request this.

The foregoing has shown that, vis-à-vis the other countries, the Netherlands has laid down a very detailed inspection procedure. Our inventory shows that four out of five countries test technical tools before being purchased and deployed. However, it is unclear how far-reaching this test is and to what extent data quality plays a key role in this test. Furthermore, the focus of safeguards in these countries lies in the final stage of the deployment of the hacking power. After the deployment of the hacking power,

the data quality could be called into question in court. In principle, the testing in the Netherlands is to ensure that data quality is not called into question.

Scenario's

Based on our research, we have formulated three scenarios which could potentially complement the way in which the Netherlands deals with technical tools and data collected by means of the hacking power. These scenarios are described in the text below.

Scenario 1: Source code and monitoring data access

Our research shows that it is required by law in Switzerland that it must be made possible to check the source code of the technical tool if so requested by the court. It must also be ensured that suppliers cannot access the data when these are being collected. These issues specifically form an obstacle in the Netherlands in inspecting commercially technical tools. It has not become clear to what extent the Swiss authorities have actually been able to fulfil both requirements. As far as is known, there has not yet been a case in which the source code was actually requested. In principle, suppliers do not benefit from giving access to their source codes. The software's working method is a well-kept secret. However, if Switzerland has succeeded in finding a workable solution, it is worth considering whether the police, public prosecutors and policymakers in the Netherlands can also achieve this in a similar manner. This could resolve two major bottlenecks in the testing procedure in the Netherlands.

Scenario 2: Changing supervisory role

During the Dutch legislative process, supervision during the exercise of the power has been an important point of discussion. Extra supervision would be necessary because judges would not always be able to properly assess the evidence collected. It was also expected that a (large) portion of the cases would never be trialled by a court. It has been suggested to set up a body comparable to the Supervisory Committee of the Intelligence and Security Services (CTIVD). Over the years, various authors have pointed to the importance of (additional) supervision or a different form of supervision. In the end, the legislator did not opt for a committee comparable to the CTIVD. Arguments for this were the existing supervision by an examining magistrate and supervision by the Central Review Committee of the Public Prosecution Service. Instead, the Justice and Security Inspectorate has been chosen, which supervises cases that are and are not submitted to the court.

Based on our research, we do not take a position on this discussion. However, it is worth noting that if the role of oversight for hacking power is explored further, there are a number of countries that have surfaced from the study that may provide guidance.

Firstly, it is relevant in this context that Belgium and France have examining magistrates overseeing the execution of the hacking power. The Examining Magistrate granting authorisation for the deployment of the hacking power also supervises the execution thereof. If needed, the Examining Magistrate may decide to terminate the hacking operations. This oversight goes beyond the role of the Examining Magistrate in

the Netherlands, who principally only oversees the hacking power prior to deployment. The working method in Belgium and France solves the problem that part of the cases are not presented to court. As a side note, it should be noted that the examining magistrates rely on the information provided. The question is thus whether this judicial oversight actually results in a substantive review during deployment. It does however offer a perspective that deviates from the Dutch system in which the Examining Magistrate grants an authorisation prior to the deployment and thereafter generally no longer oversees the hacking operations.

Secondly, also relevant is the Swedish supervisor SIN. This supervisor specifically oversees the execution of the hacking power. It is therefore similar to the Committee modelled on the CTIVD as proposed by some authors. As yet, SIN's supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness and it oversees both the police activities as well as those of the Public Prosecution Service. As such, it distinguishes itself from the tasks of the Inspectorate in the Netherlands, which only oversees the police. SIN can furthermore issue public statements in individual cases upon request or on its own accord. Given that SIN focuses both on the legal and process-related aspects, this solves the issues raised earlier that not all cases are heard by a session judge and that the judge is not always sufficiently capable of properly assessing the evidence.

Scenario 3: Customised inspection

As previously discussed, the testing in the Netherlands constitutes an important safeguard in the deployment of technical tools and the quality of the data collected by means of the tools. Practice shows that the testing and the use of technical tools do not always proceed as intended by law. Technical tools that are mainly used are tools that are not pre-approved and technical tools that cannot be approved due to their nature. Remarkably, the safeguards relating to technical tools and the data quality are less detailed by law abroad than in the Netherlands. In that respect, it is easier to deploy the hacking power abroad. Another striking aspect is that there is little or no case law available that challenges the use of the hacking power in these countries. This incidentally does not mean that the evidence provided by the hacking power will always be readily accepted. In many countries, the hacking power is relatively new and its use and any opinions thereof will continue to develop. Therefore, it cannot be ruled out that future rulings may still ensue that will impact the current legal framework in these countries. This does not detract from the interesting fact that several countries have chosen not to check data quality in a way that is done in the Netherlands. And that the working method in those countries has, as yet, not resulted in any fundamental discussions in the courts. It is for this reason that we have included a third scenario which takes a more customised approach to the inspection requirements, with attention to additional tactical and technical safeguards. This scenario explores (a) the use of a risk analysis for the inspection and (b) the question to what extent additional tactical and technical measures are adequately safeguarded.

Scenario 3a: Risk analysis in the inspection phase

Risk analyses form part of the decision to purchase and use technical tools in Germany. An SLB guideline addresses various themes that should be taken into consideration when it involves technical tools, such as the testing policy. A risk analysis identifies which objects pose a risk for these themes and what additional measures are needed. The different parties involved must conform to this. In the

Netherlands, the performing party Digit indicates that the Dutch National Commodity Inspectorate, as well as the underlying inspection protocol, does not take sufficient account of the fact that it could also operate on the basis of a risk analysis, namely in terms of the measures it takes when deploying a technical tool. It is particularly this risk analysis that appears to have taken centre stage in Germany. Therefore, the working method in Germany could be further explored to see what lessons can be learned from it in terms of the Dutch situation.

Scenario 3b: Assurance of additional tactical safeguards in the Netherlands

As noted, the Netherlands currently mainly uses technical tools that, according to the Public Prosecutor, cannot be approved due to their nature. Tactical and technical measures are taken to safeguard the data quality in this situation. There are no indications at present that the use of commercial products will be terminated. The current Minister considers this to be a 'reality that we have to deal with', as evidenced by the committee debate on 7 July 2022. The use of risk analyses described in scenario 3a may serve as a guideline to take appropriate additional measures to ensure data quality. If the working method with commercial products remains the rule rather than the exception and the method will be continued by exactly the same token, it will also be important to review the role of the Public Prosecution Service with regard to the additional safeguards, tactical or otherwise. At present, the Public Prosecution Service is the only one checking these safeguards prior to a deployment. A tactical public prosecutor leading the criminal investigation is in principle ultimately responsible for the tactical safeguards. These are also reviewed by the Digit public prosecutor and the Central Assessment Committee of the Public Prosecution Service. Owing to the sole involvement of the Public Prosecution Service and no other independent bodies, it is useful to explore which other party can (additionally) verify the adequacy of these measures, especially when a case is not presented to court.

Literatuur

Algemeen

Boeije, H. (2007). *Analyseren in kwalitatief onderzoek: Denken en doen*. Boom Onderwijs.

Berndsen, M. (2022, 17 september 2022). Twitter. www.twitter.com/cyberadvocaat/status/1571149854180782081.

Buruma, Y. (2016). *De criminele homo digitalis,* NJB 2016/1073, afl. 22, 1534-1541.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*.

Corstens, G. J. M., Borgers, M. J., & Kooijmans, T. (2018). *Het Nederlands strafprocesrech*t. (9de dr.). Wolters Kluwer.

Det Kongelige Justig- og Beredskapsdepartement (2016). *Prop. 68 L (2015–2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler).* Geraadpleegd op 24 april 2023: www.regjeringen.no/no/dokumenter/prop.-68-l-20152016/id2479232/.

Det Uafhængige Tilsyn med Bevismidler (z.d.). *Velkommen til Det Uafhængige Tilsyn med Bevismidler*. Geraadpleegd op 24 april 2023: www.bevismiddeltilsynet.dk/.

Eurojust (2016). *Cybercrime Judicial Monitor*. Geraadpleegd op 29 maart 2023: www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016-11_CJM-2_EN.pdf.

Eurojust (z.d.). *European Judicial Cybercrime Network*. Geraadpleegd op 29 maart 2023: www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network.

Eurojust (z.d.). *Mission*. Geraadpleegd op 29 maart 2023: www.eurojust.europa.eu/about-us/organisation/mission.

Fedorova, M. I., Te Molder, R. M., Dubelaar, M. J., Lestrade, S. M. A., & Walree, T. F. (2022). *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het werken van persoonsgegevens voor strafvorderlijke doeleinden*. Radboud University Press.

Gutheil, M., Liger, Q., Heetman, A., Eager, J., & Crawford, M. (2017). *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Policy Department for Citizens' Rights and Constitutional Affairs. Geraadpleegd op 29 maart 2023: www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

Hildebrandt, M. (2016). Data-gestuurde intelligentie in het strafrecht. In E. M. L. Moerel, J. E. J. Prins, M. Hildebrandt., T. F. E, Tjong Tjin Tai, G. J. Zwenne & A. H. J. Schmidt. (Red.), *Homo Digitalis, Handelingen 146e NJV vergadering 2016* (pp. 137-240). Kluwer.

Hirsch Ballin, M. F. H. & Oerlemans, J-J. (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, *1*(2), 18-38.

Home Office (2018). *Equipment interference: Code of practice*. Geraadpleegd op 24 april 2023: www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International, 2*, 1-6.

Inspectie JenV (Justitie en Veiligheid) (2020). *Verslag toezicht wettelijke hack-bevoegdheid politie 2019: Verslag van het toezicht door de Inspectie Justitie en*

Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de wet Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen. Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019.

Inspectie JenV (Justitie en Veiligheid) (2021). *Verslag toezicht wettelijke hackbevoegdheid politie 2020: Heeft de politie zich aan de regels gehouden bij het toepassen van de bevoegdheid tot binnendringen in een geautomatiseerd werk?* Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020.

Inspectie JenV (Justitie en Veiligheid) (2022). *Verslag toezicht wettelijke hackbevoegdheid politie 2021: Toezicht op de toepassing door de politie van de bevoegdheid tot het binnendringen en doen van onderzoek in een geautomatiseerd werk*. Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2022/05/31/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2021.

Ministerio Fiscal (2019). *Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos*. Geraadpleegd op 24 april 2023: www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244.

Mayer, J. (2018). Government hacking. *The Yale Law Journal,* 570-662.

Oerlemans, J-J. (2018). *Beschouwing rapport Commissie-Koops: Strafvordering in het digitale tijdperk*. Platform Modernisering Strafvordering november 2018. DOI: 10.5553/PMSV/258950952018001018001.

Jurić, M., & Roksandić, S. (2021). Croatia. In: Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis. *Duncker & Humblot,* 373-419.

Schermer, B. W. (2017). *Software Agents, Surveillance, and the Right to Privacy: A Legislative Framework for Agent-enabled Surveillance.* Leiden University Press.

Sommer, P. (2022). Evidence from hacking: A few tiresome problems. *Forensic Science International, 40*, 1-7.

Van Uden, A., & Van den Eeden, C. A. J. (2022). *De hackbevoegdheid in de praktijk: Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid* (artikelen 126nba, 126uba, 126zpa Sv). WODC. Cahier 2022-8. www.repository.wodc.nl/handle/20.500.12832/3202.

Verdelho, P. (2021). Portugal. In U. Sieber & N. von zur Muhlen (Red.), *Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (pp. 1221-1281). Duncker & Humblot. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Reihe S: Strafrechtliche Forschungsberichte (MPIS), Volume 156.

Verrest, P. A. M., & Mevis, P. A. M. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering*. Boom Juridisch.

België

Belgisch Staatsblad (2018, 19 november). *Publicatie overeenkomstig artikelen 472 tot 478 van de programmawet van 24 december 2002, gewijzigd door de artikelen 4 tot en met 8 van de wet houdende diverse bepalingen van 20 juli 2005*.

Comité P (z.d.). *Ons mission statement*. Geraadpleegd op 14 december 2022: www.comitep.be/mission-statement.html.

Conings, C. (2020, 26 februari). Grondwettelijk hof en Cassatie op één lijn: Bevel aan verdachte tot overhandiging van digitale toegangssleutel is wettig. *De Juristenkrant.*

Etsi (2020). *Etsi, the essentials*. Geraadpleegd op 29 maart 2023: www.etsi.org/images/files/Brochures/ETSI-essentials.pdf.
Etsi (z.d.). *Etsi in Europe*. Geraadpleegd op 29 maart 2023: www.etsi.org/about/etsi-in-europe.
Etsi (z.d.). *Standards*. Geraadpleegd op 29 maart 2023: www.etsi.org/standards#page=1&search=lawful%2Binterception&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-03-28&harmonized=0&keyword=&TB=386,,180&stdType=&frequency=&mandate=&collection=&sort=1.
Jobpol.be (z.d.). *Jobs als burger (CALog).* Geraadpleegd op 31 mei 2023: https://www.jobpol.be/nl/jobs-als-burger-calog
Kerkhofs, J., & Van Linthout, P. H. (2019). *Cybercrime 3.0.* Politeia.
Memorie van toelichting bij wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties. 8 juli 2016. Parl*. St.* Kamer 2015-16, nr. 54 1966/001. Geraadpleegd op 17 november 2022: www.dekamer.be/FLWB/PDF/54/1966/54K1966001.pdf.
Ministère public (z.d.). *Over ons*. Geraadpleegd op 14 december 2022: www.om-mp.be/fr/uw-om/parketten-arbeidsauditoraten-generaal/gent/parketten/over-ons.
Royer, S., & Yperman, W. (2020). Bewijsverzameling in digitale omgeving door politieambtenaren. In C. De Poot, E. Lievens, W. Stol & L. De Kimpe. (Red.), *Politie en Cybercrime*. Gompel & Svanica. *Cahier Politiestudies,* 2020/3, 23-37.
Strafwetboek België. Geraadpleegd op 20 december: www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=1867060801.
Traest, P. H. (2019). België. In: P. A. M. Verrest, & P. A. M. Mevis. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering*. Boom Juridisch. 19-80.
Yperman, W., Royer, S., & Verbruggen, F. (2019). Vissen op de grote datazee: Digitale informatievergaring in vooronderzoek en strafuitvoering. *Nullum Crimen: Tijdschrift voor Straf- en Strafprocesrecht 2019*(5). 389-416.
Wetboek van Strafvordering België. Geraadpleegd op 20 december: www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=nl&nm=1808111701&la=N.

Duitsland

BKA (z.d.). *Quellen-TKÜ und Online-Durchsuchung*. Geraadpleegd op 12 januari 2023: www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.
BKA (2018). *Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online Durchsuchung (Stand 05. Oktober 2018).* Geraadpleegd op 12 januari 2023: www.polizei.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.html.
Bundesamt für Justiz (z.d.). *Statistiken der Rechtspflege*. Geraadpleegd op 3 januari 2023: www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152.
Bundesministerium des Innern (2017). *Erlass über die Errichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich. Vom 6. April 2017*. Geraadpleegd op

31 maart 2023: www.zitis.bund.de/DE/WerWirSind/_documents/ministerialerlass_ZITiS.pdf?__blob=publicationFile&v=3.
Bundesministerium der Justiz (z.d.). *Aktuelle Gesetzgebungsverfahren*. Geraadpleegd op 31 maart 2023: www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Gesetz_zur_effektiveren_und_praxistauglicheren_Ausgestaltung_des_Strafverfahrens.html.
Bundesverfassungsgericht (z.d). *Headnotes to the Judgment of the First Senate of 27 February 2008*. Geraadpleegd op 31 maart 2023: www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.
Deutscher Bundestags (2017). *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (Drucksache 18/12785).* Geraadpleegd op 25 januari 2023: www.dserver.bundestag.de/btd/18/127/1812785.pdf.
Fedorova, M. I., Te Molder, R. M., Dubelaar, M. J., Lestrade, S. M. A., & Walree, T. F. (2022). *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het werken van persoonsgegevens voor strafvorderlijke doeleinden*. Radboud University Press.
Flade, F. (2018, 2 februari). *Ministerium gibt neuen Bundestrojaner für den Einsatz frei*. Welt. Geraadpleegd op 21 april 2023: www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html.
Groothuis, M. (2008). Bundesverfassungsgericht stelt grenzen aan online doorzoeken van personal computers. *NCJM-Bulletin, 33*(7), 990-1004.
Klip, A., Peristeridou, C. & De Vocht, D. (2019). *Citius, altius, fortius - Sneller, hoger, sterker: Wat we van Engeland en Duitsland kunnen leren in het kader van modernisering Strafvordering*. Maastricht University.
Lindemann, M. & Van Toor, D. (2018). Protection of a suspect's privacy in criminal procedures. *Ars Aequi, 67*(5), 376-384.
Meister, A. (2018, 26 juni). *Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen*. Netzpolitik.org. Geraadpleegd op 21 april 2023: www.netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/.
Niedernhuber, T. (2018). Die StPO-Reform 2017 – wichtige Änderungen im Überblick. *Juristische Arbeitsblätter, 50*(3), 169-175.
Singelnstein, T., & Derin, B. (2017). Das Gesetz zur effektiveren undpraxistauglicheren Ausgestaltung des Strafverfahrens: Was aus der stPO Reform geworden ist. *Neue Juristische Wochenschrift, 70*(37), 2646-2652.
Škorvánek, I., Koops, B-J., Newell, B. C. & Roberts, A. (2020). 'My computer is my castle': New privacy frameworks to regulate police hacking. *BYU Law Review, 2019*(4), 997-1082.
Soiné, M. (2018). Die strafprozessuale Online-Durchsuchung. *Neue Zeitschrift FürStrafrecht, 38,* 497-504.
Struijk, S. (2018). De betrokkenheid van de rechter bij de tenuitvoerlegging van straffen. In P. A. M. Verrest, & P. A. M. Mevis (Reds.), *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering* (pp. 487-538). Boom Juridisch.
Techopeda. (2016). *Software Library*. Geraadpleegd op 31 maart 2023: www.techopedia.com/definition/3828/software-library.
Zitis (z.d.). *Who we are: What else*. Geraadpleegd op 31 maart 2023: www.zitis.bund.de/EN/Home/home_node.html.

Frankrijk

Goodwin, B. (2022). *French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation*. Geraadpleegd op 17 april 2023: www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy.

Mattatia, F. (2015). Faut-il dépénaliser les hackers blancs? *Revue de science criminelle et de droit pénal comparé*, 4, 837-846.

Ministère de la Justice - Direction des affaires criminelles et des grâces (2019). *Fiche criminologique, juridique ou technique: Captation de données informatiques.*

Verrest, P. A. M. (2018). Frankrijk. In: P.A.M Verrest & P.A.M Mevis. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering* (pp. 19-80). Boom Juridisch.

Zweden

Cameron, I. (2021). Sweden. In U. Sieber, U. & N. von Zur Mühlen, N*. (Red.), Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (pp. 1343-1378)*.* Duncker & Humblot.

Klamberg, M. (2020). *Evidentiary Matters in the Context of Investigating and Prosecuting International Crimes in Sweden: Admissibility, Digital Evidence and Judicial Notice*. Faculty of Law, Scandinavian Studies in Law. Stockholm University Research Paper No. 85

Wong, C. (2012*). Overview of Swedish Criminal Procedure*. Geraadpleegd op 11 juni 2023: www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_10/spl_85/pdfs/24.pdf

Zwitserland

Bundesgerichtsentscheid (BGE). *Urteilskopf. 138 IV 232*. Geraadpleegd op 4 mei 2023: www.relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F138-IV-232%3Ade&lang=de&type=show_document.

Basanisi, M. (2019). GovWare – Legiferierung und grundrechtliche Herausforderungen Geheime Überwachung verschlüsselter Kommunikation im Kontext der neuen Schweizer Gesetzgebung zum Einsatz besonderer Informatikprogramme nach Art. 269ter und Art. 269quater StPO. *Jusletter* 14 janvier 2019.

Betschman, S., & Murer Mikolásek, A. (2018). Anwendungsmöglichkeiten von GovWare. *AJP/PJA 6/2018*, 748-752. Geraadpleegd op 17 april 2023: www.betschmann.ch/AJP_Anwendungsm%C3%B6glichkeiten_von_GovWare.pdf.

Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Geraadpleegd op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/31/de.

Eidgenössische Justiz- und Polizeidepartement (EJPD) (2019, 27 februari). *Besondere Informatikprogramme: die Kosten werden geteilt*. Geraadpleegd op 29 maart 2023: www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2019/2019-02-27.html.

Eidgenössische Justiz- und Polizeidepartement (EJPD) (2019b). *Erläuterungen zur Revision der Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei (Gebührenverordnung fedpol, GebV-fedpol)*. Geraadpleegd op 29 maart 2023: www.digitale-gesellschaft.ch/uploads/2020/01/erl-vo-d.pdf.

Eidgenössische Justiz- und Polizeidepartement (EJPD) (2022). *Statistik*. Geraadpleegd op 29 maart 2023: www.li.admin.ch/de/stats.
Eidgenössische Justiz- und Polizeidepartement (EJPD) (2023). *Häufig gestellte Fragen FAQ - Bundestrojaner/GovWare*. Geraadpleegd op 29 maart 2023: www.li.admin.ch/de/dokumentation/faq.
Engler, S. (2015). Speech Engler Stefan. In: *Amtliches Bulletin – Ständerat. Wintersession 2015. Fünfte Sitzung. 07.12.15. 15h15. 13.025.* Geraadpleegd op 3 mei 2023: www.parlament.ch/en/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-videos?TranscriptId=192170.
Fedlex (2017, 11 januari). *Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei (Gebührenverordnung fedpol, GebV-fedpol).* Geraadpleegd op 23 maart 2023: www.fedlex.admin.ch/eli/oc/2017/60/de.
Godenzi, G. & Caprara, T. (2018). Zwitserland. In P.A.M. Verrest & P.A.M. Mevis (Red.), *Rechtsvergelijkende inzichten voor de moderinisering van het Wetboek van Strafvordering* (pp. 281-332). Boom Juridisch.
Hansjakob, T. (2011). Einsatz von GovWare – zulässig oder nicht? *Jusletter* 5.12.2011, N 16, 30. Geraadpleegd op 29 maart 2023: www.hansjakob.ch/thomas/jusletter_einsatz_govware.pdf.
ProDemos (2022, februari). *Zwitserland*. Geraadpleegd op 29 maart 2023: www.prodemos.nl/app/uploads/2023/01/webdossier-Kiesstelsel-Zwitserland-versie-oktober-2022.pdf.
Schweizerisches Strafgesetzbuch. Geraadpleegd op 29 maart 2023: www.fedlex.admin.ch/eli/cc/54/757_781_799/de.
Verordnung des EJPD vom 15. November 2017 über das beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs (VBO-ÜPF). Geraadpleegd op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/33/de.
Verordnung des EJPD vom 15. November 2017 über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF). Geraadpleegd op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/35/de.
Verordnung vom 15. November 2017 über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF). Geraadpleegd op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/36/de.
Verordnung vom 15. November 2017 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF). Geraadpleeg op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/34/de.
Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). Geraadpleegd op 17 april 2023: www.fedlex.admin.ch/eli/cc/2018/32/de.

Bijlage 1 Bronnenoverzicht

Tabel B1.1 Geraadpleegde bronnen per land

Landen	Interviews					Litera-tuur	Wetge-ving/ beleid	Euro-just
	OM	Politie	Mini-sterie	Weten-schap	Overig			
Australië				X		X	X	
België	X		X	X		X	X	
Bulgarije								X
Canada				X		X	X	
Duitsland		X		X	X	X	X	X
Denemarken			X*	X		X	X	
Estland	X*						X	
Finland					X		X	
Frankrijk		X*	X			X	X	X
Griekenland					X		X	
Hongarije	X*					X	X	
Ierland				X		X	X	
Italië				X			X	X
Kroatië	X*		X*	X		X	X	
Letland								X
Litouwen	X			X			X	X
Luxemburg	X						X	
Noorwegen		X					X	X
Oostenrijk						X		X
Polen				X			X	
Portugal	X*			X		X	X	X
Roemenië	X						X	
Slovenië				X				X
Slowakije				X*			X	X
Spanje				X		X	X	X
Tsjechië	X*			X			X	
Verenigd Koninkrijk				X		X	X	X
Verenigde Staten				X		X	X	
Zweden	X	X	X		X*		X	
Zwitserland	X	X	X*			X	X	X

* Betreft een vragenlijst per mail.

Bijlage 2 Landenoverzicht hackbevoegdheid

Tabel B2.1 Landenoverzicht hackbevoegdheid

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
Australië	Division 5 & 6 Surveillance Apparatuur Wet (SAW). Afdeling 2 Misdadenwet 1914 (A2M).	Direct	Misdrijven met een gevangenisstraf van twee jaar of meer en (1) een *commonwealth* misdrijf is, (2) een misdrijf tegen de staat is, (3) een misdrijf tegen een wet van een territorium en dat niet te kwalificeren is als een serieus terroristisch misdrijf (Part IAA, Division 1, 3C Interpretation, A2M).	Verstoren van data om criminele feiten te voorkomen of stoppen (zoals offline halen van kinderporno) (divisie 5 SAW), monitoren van netwerkactiviteit om inzicht te krijgen in criminele netwerken (divisie 6 SAW) en het overnemen van een account (Part IAAC, A2M).	Voor zover bekend niet.
België	Artikelen 89ter en 90ter Wetboek van Strafvordering.	Direct	Lange lijst met misdrijven opgesomd in artikel 90ter paragraaf 2 Sv, waaronder: aanslag op het leven of de persoon van de koning (art. 101 Sr), het opnemen van niet-publiek toegankelijke communicatie zonder toestemming (art. 314bis Sr) en doodslag om afpersing of diefstal te vergemakkelijken (art. 475 Sr).	Artikel 89ter Sv: Doorzoeken van geautomatiseerde werken. Er mogen geen gegevens worden vastgelegd, behalve een 'staal' ter illustratie (vergelijkbaar met het nemen van een staal drugs bij een huiszoeking). Artikel 90ter Sv: Geen beperking op het type gegevens en het doorzoeken en vastleggen ervan. Dit betekent dat de meeste onderzoekshandelingen kunnen worden verricht, zoals de interceptie van communicatie, het aanzetten van een microfoon en camera (surveillance) en het bevragen van de locatie.	Wat betreft de beschikbare jurisprudentie wordt het hacken zelf zelden ter discussie gesteld in de rechtszaal (persoonlijke communicatie, 24 maart 2023).
Bulgarije	Geen wettelijke bevoegdheid.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Canada	Artikel 487.01 Wetboek van Strafrecht.	Indirect	Geen beperking op het type misdrijven volgens artikel 487.01 lid 1 sub a Sr. Het is aan de rechter om te beoordelen of het middel kan worden ingezet.	Geen explicitering van de onderzoekshandelingen die zijn toegestaan. Een rechter dient toestemming te geven voor de onderzoekshandelingen die verricht gaan worden. Het kan gaan om zowel opgeslagen als stromende gegevens.	Voor zover bekend niet.
Denemarken	Artikel 791b en 799 Wet op de Rechtspleging (WodR).	Direct	Artikel 791b WodR: strafbare feiten waarop een gevangenisstraf van zes jaar of meer staat of die een schending vormen van hoofdstuk 12 of 13 van het Wetboek van Strafrecht, zoals terrorisme of misdrijven tegen de Grondwet. Artikel 799 WodR: lange lijst aan misdrijven genoemd in lid 1. Onder meer: misdrijven tegen de autonomie en veiligheid van de staat, ernstige drugsgerelateerde misdrijven en kinderpornografie.	Artikel 791b WodR: gegevensuitlezing. Artikel 799 WodR: heimelijke zoeking. Geen specifieke handelingen beschreven in de wet.	Op 10 mei 2012 oordeelde het Hooggerechtshof dat de politie die wachtwoorden gebruikt van Facebook en berichtendiensten van een verdachte valt onder de regels van een herhaalde heimelijke zoeking (Justitieel wekelijks tijdschrift, U 2012.2614 H).

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
Duitsland	Artikelen 100a en 100b Wetboek van Strafvordering.	Direct	Artikel 100a Sv: lange lijst met misdrijven genoemd in lid 2. Gaat om 'ernstige' misdrijven zoals: afpersing, drugsgerelateerde misdrijven en witwassen. Artikel 100b Sv: lange lijst aan misdrijven genoemd in lid 2. Gaat om 'zeer ernstige' misdrijven en voorbereidende handelingen zoals: georganiseerde criminaliteit, moord met verzwarende omstandigheden en mensenhandel.	Artikel 100a Sv: bronintercepte van telecommunicatie. Artikel 100b Sv: doorzoeken en vastleggen van alle gegevens op een geautomatiseerd werk (online doorzoeking).	Beslissing van het Grondwettelijk Hof uit 2008: gaat onder andere over de splitsing tussen artikelen 100a en 100b Sv. (Bundesverfassungsgericht, z.d.).
Estland	Artikel 126-1 Wetboek van Strafvordering.	Indirect	Lange lijst met misdrijven opgesomd in artikel 126-2 Sv. Onder meer: moord, vrijheidsontneming en witwassen.	In beginsel geen restricties op type handelingen, is afhankelijk van de machtiging van de rechter.	Voor zover bekend niet.
Finland	Hoofdstuk 10 sectie 23 Wet Dwangmiddelen (WD) (*Pakkokeinolaki*).	Direct	Op basis van hoofdstuk 10 sectie 16 WD gaat het om misdrijven waarvoor een gevangenisstraf van minstens vier jaar kan worden opgelegd, drugsdelicten, voorbereidende handelingen van terrorisme, verzwarend douanedelict, voorbereidende handelingen van gijzeling en voorbereidende handelingen voor een gewelddadige overval.	Doorzoeken en vastleggen van gegevens en interceptie van communicatie.	Voor zover bekend niet.
Frankrijk	Artikel 706-95-11 tot 706-102-5 en artikel D 15-1-6 Wetboek van Strafvordering.	Direct	Terrorisme, georganiseerde criminaliteit (art. 706-73 Sv) en zware economische criminaliteit (art. 706-73-1 Sv).	Zowel opgeslagen als stromende gegevens kunnen worden vastgelegd (art. 706-102-01 Sv). Voorbeelden zijn tekst, afbeeldingen en audio (Fiche juli 2019, p. 1-2).	Constitutionele toetsing (Le conseil constitutionnel, beslissing van 8 april 2022) & Encrochat (oa Le cour de cassation, 11 oktober 2022)
Griekenland	Geen wettelijke bevoegdheid.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Hongarije	Artikel 232 lid 1 Wetboek van Strafvordering. De politie kan dit niet zelf doen. De nationale Veiligheidsdienst doet dit op verzoek van organisaties uit de strafrechtsketen, zoals de politie of het Openbaar Ministerie.	Direct	Lange lijst met misdrijven genoemd in artikel 234 Sv. Onder meer: misdrijven waarvoor een gevangenisstraf van vijf jaar of meer kan worden opgelegd of specifieke misdrijven die staan opgesomd in lid 2 en 3, zoals seksueel misbruik, corruptie en handel met voorkennis. Kan ook worden ingezet indien sprake is van voorbereidingshandelingen (zie lid 4).	Toegang krijgen tot en opslaan van gegevens afkomstig uit een geautomatiseerd werk (heimelijke surveillance) (art. 232 lid 1 Sv). Onderscheppen van communicatie (art. 232 lid 5 Sv).	Voor zover bekend niet.
Ierland	Surveillance Wet 2009. Het is onbekend in hoeverre deze wet ook daadwerkelijk voor de hackbevoegdheid wordt ingezet.	Indirect	Op basis van artikel 2 Wetboek van Strafrecht gaat het om misdrijven (inclusief voorbereiding daarvan) waarvoor een gevangenisstraf van vijf jaar of meer kan worden opgelegd.	Geen specifieke handelingen beschreven in de wet. Wel zijn de volgende handelingen op basis van de Wet op het onderscheppen van postpakketten en telecommunicatieberichten 1993 uitgesloten: interceptie van telecommunicatie, tekstberichten en e-mail.	Voor zover bekend niet.
Italië	Artikelen 266 en 267 Wetboek van Strafvordering.	Direct	Lange lijst aan misdrijven genoemd in artikel 266 Sv. Onder meer: misdrijven waarvoor een gevangenisstraf van vijf	Interceptie van communicatie op een draagbaar elektronisch apparaat. Ook kan een microfoon op specifieke momenten worden aangezet op	Tot de introductie van de bevoegdheid in 2017 is er veel jurisprudentie beschikbaar.

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
			jaar of meer kan worden opgelegd, drugsdelicten, smokkel en wapendelicten.	een draagbaar elektronisch apparaat (surveillance).	Door de komst van de bevoegdheid is deze jurisprudentie achterhaald. Sinds de introductie van de nieuwe bevoegdheid is er één uitspraak geweest die bevestigt dat de inzet van de huidige bevoegdheid rechtmatig is (persoonlijke communicatie, 12 mei 2022).
Kroatië	Artikel 332 Wetboek van Strafvordering.	Indirect	Lange lijst met misdrijven genoemd in artikel 334 Sv. Onder meer misdrijven waarvoor een gevangenisstraf van vijf jaar of meer kan worden opgelegd. Bijvoorbeeld terrorisme, kindermisbruik en witwassen.	Monitoren en technische opname van telefoongesprekken en andere middelen die *remote* technische communicatie mogelijk maken (art. 332 (1)(1) Sv). Onderscheppen, verzamelen en opnemen van computerdata (art. 332 (1)(2) Sv). Toegang verschaffen tot een terrein zodat daar surveillance en technische opnames van het terrein kunnen plaatsvinden (art. 332 (1)(3) Sv). Heimelijk volgen van individuen en objecten en technische opnames maken van beide (art. 332 (1)(4) Sv).	Voor zover bekend niet.
Letland	Geen wettelijke bevoegdheid.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Litouwen	Artikel 158 Wetboek van Strafvordering en artikel 10 Wet criminele intelligence (Wci).	Indirect	Artikel 158 Sv: misdrijven waarvoor een gevangenisstraf van meer dan drie jaar opgelegd kan worden. Artikel 10 Wci: misdrijven waarvoor een gevangenisstraf van meer dan zes jaar kan worden opgelegd, verschillende misdrijven waarvoor een gevangenisstraf van meer dan drie jaar kan worden opgelegd, voorvluchtige personen, vermiste personen, beveiliging personen en preventie activiteiten van criminele organisatie.	Artikel 158 Sv: geen explicitering van onderzoekshandelingen. In het bevel dienen de acties opgenomen te worden die mogen worden uitgevoerd (art. 158 (3) Sv). Artikel 2 lid 22, 8 en 10 Wci: geen explicitering van onderzoekshandelingen.	Voor zover bekend niet.
Luxemburg	Artikel 88-1 lid 3 Wetboek van Strafvordering	Direct	De bevoegdheid is op basis van artikel 88-2 lid 1 Sv beperkt tot misdrijven tegen de staat, terrorisme en financiering van terrorisme.	Het is alleen mogelijk om live input en output te tappen van een gebruiker zoals die worden weergegeven op het scherm (art. 88-1 Sv).	Voor zover bekend niet.
Noorwegen	Artikel 216o in samenhang met artikel 216p Wetboek van Strafvordering.	Direct	Opsomming van misdrijven in artikel 216o lid 1 Sv. Onder meer: misdrijven waarvoor een gevangenisstraf van tien jaar of meer kan worden opgelegd (sub a) en misdrijven die staan opgesomd in sub b, zoals openbaarmaking van staatsgeheimen, deelname aan een terroristische organisatie en mensenhandel.	Het vastleggen van niet-publiekelijk beschikbare gegevens in een geautomatiseerd werk. Dit omvat communicatie, elektronisch opgeslagen gegevens en andere informatie over het gebruik van een geautomatiseerd werk of van een gebruikersaccount (art. 216o lid 1 en 4 Sv). Gaat onder andere om de volgende handelingen: opnemen van audio via microfoon, opnemen van audio op geautomatiseerd werk, opnemen van video via camera, keylogging, bevragen van opgeslagen gegevens, interceptie van internetgegevens en	Voor zover bekend niet.

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
				metadata (Det Kongelige Justig- og Beredskapsdepartement, 2016 (Wetsvoorstel)).	
Oostenrijk	Geen wettelijke bevoegdheid.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Polen	Artikel 19 lid 6 sub 4 Politiewet (Pw)	Direct	Lange lijst van misdrijven opgesomd in artikel 19 lid 1 Pw. Onder meer: moord en doodslag, mensenhandel en kinderporno.	In artikel 19 lid 6 Pw wordt beschreven welke handelingen mogen worden verricht: interceptie van communicatie, aanzetten van microfoon en camera in specifieke ruimtes (surveillance), doorzoeken en vastleggen van opgeslagen communicatie, doorzoeken en vastleggen van gegevens uit geautomatiseerde werken en toegang krijgen tot en doorzoeken van een e-mailbox.	Voor zover bekend niet.
Portugal	Artikel 19 Cybercrimewet, artikel 187 Wetboek van Strafvordering in samenhang met artikel 188 en 189 en Wet nr. 05/2002. Deze artikelen zijn leidend, maar de reikwijdte ervan worden door sommige auteurs ter discussie gesteld (persoonlijke communicatie, 15 juni 2023).	Indirect	Artikel 19 Cybercrimewet: lijst van misdrijven die vastgelegd zijn in de Cybercrimewet en andere vormen van criminaliteit die gepleegd worden met behulp van een geautomatiseerd werk en die bestraft kunnen worden met een gevangenisstraf van tenminste vijf jaar. Daarnaast wordt een aantal andere misdrijven genoemd, los van hun mogelijke bestraffingsmogelijkheid, met inbegrip van misdrijven tegen minderjarigen en personen met een handicap die de seksuele vrijheid en zelfbeschikking belemmeren, fraude met verzwarende omstandigheden en andere economische en financiële misdrijven, discriminatie op grond van ras, godsdienst of geslacht en misdrijven in verband met inbreuken op het auteursrecht en verwante rechten. Artikel 187 Sv: opsomming van diverse misdrijven, onder meer misdrijven die met een gevangenisstraf van tenminste drie jaar of meer kunnen worden bestraft, drugsgerelateerde misdrijven, kidnapping en gijzeling en misdrijven tegen staatsveiligheid. Wet 05/2002: diverse misdrijven vastgelegd in artikel 1 lid 1 t/m 4. Onder andere: drugshandel, terrorisme, corruptie, wapenhandel, witwassen en kinderpornografie (art. 1 lid 1 Wet 05/2002).	Artikel 19 Cybercrimewet: activiteiten die kunnen worden uitgevoerd op basis van artikel 19 van de Cybercrimewet staan niet geëxpliciteerd in de wet (Verdelho, 2021, p. 1260-1261). Artikel 187 Sv: Onderscheppen en opnemen van telefoongesprekken en communicatie (art. 187 lid 1). Wet 05/2002: Registreren van geluid en afbeeldingen (art. 6 Wet nr 05/2002).	Voor zover bekend niet.
Roemenië	Artikelen 138 en 139 Wetboek van Strafvordering.	Direct	In artikel 139 lid 2 Sv worden de volgende misdrijven genoemd: misdrijven waarvoor een gevangenisstraf van vijf jaar of meer kan worden opgelegd. Daarnaast de volgende specifieke misdrijven: drugshandel, misdrijven tegen de nationale veiligheid, mensenhandel, terrorisme, witwassen, vervalsing van geld en waardepapieren, vervalsing van elektronische betalingsinstrumenten, vermogensdelicten, afpersing, verkrachting, vrijheidsontneming, belastingontduiking, corruptie, misdrijven tegen de financiële belangen van de Europese Unie en computercriminaliteit.	In artikel 138 Sv worden de volgende handelingen beschreven: (a) de interceptie van communicatie; (b) toegang krijgen tot een geautomatiseerd werk; (c) het aanzetten van een microfoon of camera (surveillance); (d) locatiebepaling en (e) het verkrijgen van informatie over financiële transacties individuen.	Voor zover bekend niet.

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
Slovenië	Geen wettelijke bevoegdheid.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Slowakije	Artikel 115 Wetboek van Strafvordering.	Direct	In artikel 115 Sv lid 1 staat een opsomming van misdrijven genoemd: corruptie, extremistische misdrijven, misbruik van het gezag van een ambtenaar, een witwasdelict zoals beschreven in de artikelen 233 en 234 Sr of een ander opzettelijk strafbaar feit dat is verbonden aan een internationaal verdrag.	Interceptie van alle vormen van communicatie (beeld, geluid en data) (persoonlijke communicatie, 8 augustus 2022).	Voor zover bekend niet.
Spanje	Artikel 588 en verder Wetboek van Strafvordering.	Direct	Lijst van misdrijven genoemd in artikel 588 lid 1 Sv. Misdrijven gepleegd door criminele organisaties, terrorisme, misdrijven gepleegd tegen minderjarigen of handelingsonbekwame personen, misdrijven tegen de Grondwet, verraad en misdrijven gerelateerd aan nationale defensie en computercriminaliteit.	Online onderzoek. Verder geen specifieke handelingen beschreven in de wet. Zie artikel 588 lid 1 Sv.	Voor zover bekend niet.
Tsjechië	Artikel 158d lid 3 Wetboek van Strafvordering.	Indirect	Geen beperking van type misdrijven opgenomen in de wet, behalve dat het moet gaan om misdrijven die opzettelijk gepleegd zijn (persoonlijke communicatie, 14 juni 2023)	Handelingen staan niet beschreven in de wet. Alles wat op een geautomatiseerd werk plaatsvindt, kan worden gemonitord (art. 158d paragraaf 2 Sv).	Voor zover bekend niet.
Verenigd Koninkrijk	Hoofdstuk 5 Wet Opsporingsbevoegdheden (WO).	Direct	Ernstige misdrijven (zie art. 106 WO). Betreft misdrijven waarvoor een gevangenisstraf van drie jaar of meer kan worden opgelegd of gedrag waarbij geweld wordt gebruikt, gedrag dat resulteert in substantieel financieel gewin of gedrag dat door een groot aantal personen wordt uitgevoerd voor een gemeenschappelijk doel (art. 263 WO).	Het verkrijgen van communicatie of andere informatie, waaronder het monitoren, observeren of luisteren naar de communicatie en andere activiteiten van een persoon, en het opnemen daarvan (art. 99 lid 2 en 4 WO).	Voor zover bekend niet.
Verenigde Staten	Geen expliciete wetgeving ten aanzien van hacking. Indien hacken wordt aangemerkt als een zoeking in het kader van het Vierde amendement, geldt Rule 41 van het federaal Wetboek van Strafvordering (persoonlijke communicatie, 27 juni 2022) en moet een bevel worden gevraagd. De helft van de rechters in de districtsrechtbanken (Škorvánek et al., 2020), die een oordeel moeten vellen over het aangevraagde bevel, ziet sommige	Deels direct	Geen beperking van het soort misdrijven.	Verschillende handelingen kunnen worden verricht, waarmee diverse soorten gegevens verzameld kunnen worden: abonneeinformatie, metadata communicatie, geolocatiegegevens, inhoud van (opgeslagen) communicatie en bestanden. Niet voor alle soorten gegevens is een bevel nodig op basis van het Vierde Amendement (Mayer, 2018; US vs Jones; Florida V Jardines; California v Riley; Škorvánek et al., 2020)	In 2011, 2013, 2014 en 2015 waren er enkele federale gerechtelijke uitspraken met betrekking tot hacken door de overheid. In 2016 en 2017 samen waren er ongeveer 100 uitspraken (Mayer, 2018). Op 5 november 2018 waren er 17 federale beslissingen van de Hoger beroep rechtbanken en talrijke federale gerechtelijke uitspraken in honderden verschillende individuele vervolgingen. Alle beslissingen hadden betrekking op twee federale opsporingsonderzoeken naar kinderporno (Škorváneket al., 2020).

Land	Artikel hackbevoegdheid	Direct/indirect bevoegdheid	Type misdrijven	Onderzoeks-handelingen	Jurisprudentie
	hackactiviteiten (afhankelijk van het soort gegevens dat wordt binnengehaald) niet als een zoeking in het kader van het Vierde amendement (Mayer, 2018).				
Zweden	Wet (2020:62) heimelijke gegevensuitlezing (Whg).	Direct	Op basis van sectie 4 Whg gaat het om misdrijven (inclusief voorbereiding) met een minimale strafmaat van twee jaar of hoger. Daarnaast worden specifiek misdrijven gerelateerd aan drugs en smokkel genoemd.	Interceptie communicatie, communicatie monitoren, locatiedata opslaan, microfoon aanzetten in specifieke ruimtes (surveillance) en overige data (als voorbeeld worden interceptie van inloggegevens genoemd) (Sectie 2 Whg).	Twee arresten waarin onder meer de kwaliteit van gegevens ter discussie wordt gesteld. Ondanks dat de gegevens onvolledig zijn oordeelt de rechtbank dat 'de berichten qua tijd en inhoud goed overeenkomen met de werkelijkheid'. In beide zaken heeft de rechtbank de bezwaren van de verdediging verworpen (Uitspraak districtsrechtbank Eskilstuna 26-02-2021 in zaak B 210-21 & Uitspraak rechtbank Stockholm d.d. 22 april 2021 in zaak nr. B 5546-20).
Zwitserland	Artikel 269ter Wetboek van Strafvordering.	Direct	Lange lijst van misdrijven genoemd in artikel 286 lid 2 Sv. Onder meer: geweldsmisdrijven, vrijheidsontneming en misdrijven tegen de seksuele integriteit.	Interceptie van telecommunicatie (alleen geluid, geen aanvullende data zoals foto's).	Voor zover bekend niet.

Bijlage 3 Landenoverzicht waarborgen verzamelde gegevens

Tabel B3.1 Overzicht waarborgen ten aanzien van gegevens verzameld met behulp van de hackbevoegdheid

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
Australië	Nee	Ombudsman houdt toezicht op uitvoering bevoegdheid.	Aanwezigheid van zogenaamde bewijscertificaten, waarin alle uitgevoerde handelingen van de uitvoerend ambtenaar zijn vastgelegd (part 6, divisie 4 SAW).	Geen informatie bekend	Data moet op een veilige plek worden opgeslagen en verwijderd worden als de zaak is afgesloten (herziene memorie van toelichting).	Geen informatie bekend	Bij gebruik bevoegdheid moet melding worden gemaakt aan inspectie, ombudsman & minister (part 6, divisie 2 SAW).
België	Nee	Niet aanwezig	Regels omtrent verslaglegging en dossiervorming (art. 46quinquies paragraaf 5 en 7 Sv; art. 90quater paragraaf 3 Sv; art. 90sexies paragraaf 1 Sv; art. 90sexies paragraaf 4; art. 90septies Sv).	Officieren van de gerechtelijke politie brengen tenminste om de vijf dagen schriftelijk verslag uit aan de onderzoeksrechter over de uit te voeren machtiging (art. 90quater paragraaf 3 Sv).	Een aantal stukken wordt onder verzegelde omslag bij de griffie neergelegd (art. 90septies paragraaf 4 Sv). Sommige gegevens dienen vernietigd te worden (art. 90septies paragraaf 3 Sv).	Iedere persoon ten aanzien van wie de bevoegdheid tot data-interceptie (art. 90ter Sv) is ingezet, dient schriftelijk in kennis te worden gesteld van de aard van de inzet van de bevoegdheid en de dagen waarop de bevoegdheid is ingezet (art. 90novies Sv). De verdachte of een advocaat kunnen verzoeken om inzage van de gegevens en een verzoek doen om (een deel van) die gegevens toe te voegen aan het dossier. Dat verzoek kan geweigerd worden (art. 90septies paragraaf 6 Sv).	Passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van (…) communicatie of gegevens van een geautomatiseerd werk te waarborgen (art. 90septies paragraaf 1 Sv).
Bulgarije	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Canada	Nee	Niet aanwezig	Verslaglegging van uitgevoerde handelingen vindt plaats in het proces-verbaal (persoonlijke communicatie, 13 juni 2022).	Geen informatie bekend	Geen informatie bekend	Nadat uitvoering is gegeven aan het bevel, dient hiervan kennis te worden gegeven, binnen een termijn die een rechter redelijk acht (art. 487.01 paragraaf 5.1 Sr). Tijdens de zitting dient informatie te worden	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
						gegeven over het bewijs dat verzameld is. Het geven van informatie geldt ten aanzien van gegevens die worden gebruikt om te laten zien dat iemand (on-)schuldig is en ten aanzien van de vraag of rechten (in '*Charter of Rights and Freedoms*') geschonden worden. Een advocaat kan de politie tijdens een zitting verhoren om te kijken of er sprake is van een dergelijke schending (persoonlijke communicatie, 13 juni 2022).	
Denemarken	Nee	De Deense Onafhankelijke Raad voor toezicht op bewijsmateriaal houdt toezicht op de wijze waarop de politie en het Openbaar Ministerie met digitaal bewijs omgaan. Het uitvoeringsproces en de kwaliteit van het digitale bewijs staan centraal. De Raad buigt zich niet over individuele zaken. Ook keurt zij geen individuele technische hulpmiddelen (Det Uafhængige Tilsyn med Bevismidler, z.d.; persoonlijke communicatie, 22 augustus 2022). Bij de gegevensuitlezing en bij de heimelijke zoeking wordt een advocaat aangesteld voor de persoon tegen wie de bevoegdheid	Geen informatie bekend	Geen informatie bekend	Geen informatie bekend	De advocaat moet genotificeerd worden van alle rechtszittingen in de zaak, mag deze bezoeken en heeft het recht om het materiaal in te zien. Hij of zij mag een kopie van het materiaal ontvangen. Als de politie van mening is dat het materiaal bijzonder vertrouwelijk van aard is en dat een kopie niet kan worden overgedragen, zal de rechtbank daar een uitspraak over doen (zie art. 791b lid 4 en art. 799 lid 2 juncto art. 785 WodR). In Denemarken geldt na afloop van de inzet van de gegevensuitlezing en van de heimelijke zoeking een notificatieplicht (tenzij uitzonderingsregels gelden) (zie art. 791b lid 4 en art. 799 lid 2 juncto art. 788 WodR).	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
		wordt ingezet, voordat de rechtbank een beslissing neemt over de inzet van de bevoegdheid. De advocaat moet de mogelijkheid krijgen een oordeel te vellen over de aangevraagde inzet alvorens de rechter een besluit neemt (zie art. 791b lid 4 en art. 799 lid 2 juncto art. 784 Wet op de Rechtspleging (WodR)).					
Duitsland	Nee	De '*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*' (ZITiS) ondersteunt en adviseert federale veiligheidsdiensten bij beveiligingstaken op het gebied van informatietechno-logie. ZITiS speelt een rol rondom (onderzoek naar en de ontwikkeling van) technische hulpmiddelen (Bundesministerium des Innern, 2017 (het Instellingsbesluit van ZITiS); persoonlijke communicatie, 21 november 2022).	Er zijn regels met betrekking tot verslaglegging wanneer een technisch hulpmiddel wordt gebruikt, zie daarvoor artikelen 100a lid 6 en 100b lid 4 Sv.	Geen informatie bekend	Technische hulpmiddelen moeten, volgens de stand van de techniek, bescherming bieden tegen ongeoorloofd gebruik door derden. Gekopieerde gegevens moeten, volgens de stand van de techniek, worden beschermd tegen wijziging, ongeoorloofde verwijdering en ongeoorloofde toegang door derden (art. 100a lid 5 Sv). De communicatieoverdracht moet plaatsvinden tussen de ophaalsoftware op het geautomatiseerd werk van de verdachte en de registratie- en controle-eenheid van de uitvoerende instantie (BKA, 2018 (SLB-richtlijn)).	In Duitsland geldt een notificatieplicht. De kennisgeving moet zo snel mogelijk plaatsvinden (tenzij uitzonderingsregels gelden) (art. 101 lid 4 Sv).	In het geval van bronintercepte moet een technisch hulpmiddel zo worden ingesteld dat het alleen lopende communicatie of de inhoud en de omstandigheden van de communicatie opneemt (art. 100a lid 5 sub 1 Sv). Technische hulpmiddelen mogen alleen wijzigingen aanbrengen aan het geautomatiseerd werk van de betrokken persoon die essentieel zijn voor de gegevensverzameling (art. 100a lid 5 sub 2 Sv). De aangebrachte wijzigingen moeten, indien technisch mogelijk, na beëindiging van de inzet van de bevoegdheid automatisch ongedaan gemaakt worden (art. 100a lid 5 sub 3 Sv). Alleen medewerkers die de bevoegdheid uitvoeren

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
							krijgen toegang tot de verzamelde gegevens. Dat moet worden gedocumenteerd. Bovendien krijgen medewerkers alleen toegangsrechten die noodzakelijk zijn voor de uitvoering van hun rol. De gebruikte software moet worden gearchiveerd (BKA, 2018 (SLB-richtlijn)).
Estland	Nee	Niet aanwezig	Alle gegevens die worden verzameld moeten worden opgeslagen in een 'bewerkingsbestand' (audio, video, data etc.). Hierin zijn de volgende elementen opgenomen: (1) naam van instantie die de inzet uitvoert, (2) tijd en plaats van de inzet, (3) naam van de betrokkene, (4) datum van het bevel, (5) alleen gegevens die relevant zijn voor waarheidsvinding (art. 126-10 t/m 126-12 Sv).	Geen informatie bekend	Geen informatie bekend	Na afronding van de heimelijke operatie worden betrokkenen in beginsel geïnformeerd. Hiervoor gelden uitzonderingen als notificatie het opsporingsonderzoek of de opsporingsmethoden kan schaden. Zodra deze beperkingen niet meer gelden moet alsnog een betrokkene worden geïnformeerd (art. 126-13 Sv). Na notificatie krijgt de betrokkene in principe inzage in het 'bewerkingsbestand' (art. 126-14 Sv).	Geen verdere informatie
Finland	Nee	Niet aanwezig	Geen informatie bekend	Geen informatie bekend	Alleen gegevens van de verdachte mogen worden opgeslagen. Andere gegevens moeten worden vernietigd (persoonlijke communicatie, 27 juni 2023).	Geen informatie bekend	Geen informatie bekend
Frankrijk	Nee	In Frankrijk is STNCJ (*'Service technique national de captation judiciaire'*) verantwoordelijk voor het ontwerp, de centralisering en de implementatie van	Gegevens die worden gebruikt voor waarheidsvinding moeten getranscribeerd worden door een ambtenaar van de gerechtelijke politie (art. 706-102-8 Sv). Er moet een rapportage	Artikel 706-95-14 Sv regelt dat de bevoegdheid wordt uitgevoerd onder verantwoordelijkheid van de betrokken rechters (afhankelijk van het onderzoek). Zij kunnen	Verkregen gegevens worden verzegeld opgeslagen (art. 706-95-18 Sv). Na het verstrijken van de verjaringstermijn worden de gegevens verwijderd op	In de wet is geen notificatieplicht opgenomen. De verdachte krijgt inzage in de gegevens die in de rechtszaak worden gebruikt.	Voor de inzet van de bevoegdheid mag (ook) gebruik worden gemaakt van middelen waarvan de werking staatsgeheim is (Fiche, juli 2019, p. 6).

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
		technische hulpmid-delen die worden gebruikt om data te onderscheppen. Hieronder vallen ook technische hulpmid-delen die de politie gebruikt voor het hacken. STNCJ is onderdeel van het DGSI, een Franse inlichtingendienst die onder het ministerie van Binnenlandse zaken valt (Fiche, juli 2019).	worden opgesteld waarin de installatie van een technisch hulpmiddel wordt beschreven. Daarin moeten onder andere de datum en het tijdstip van het begin en van het einde van de inzet worden opgenomen (art. 706-95-18 Sv).	de bevoegdheid elk moment onderbreken. Rechters dienen verder geïnformeerd te worden over de voortgang. Als blijkt dat de toestemming en de wettelijke voorschriften niet op orde zijn, kan de inzet worden gestopt (Fiche, juli 2019, p. 6).	last van de officier van justitie (Fiche juli 2019, p. 7).		
Griekenland	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Hongarije	Nee	Niet aanwezig	De inzet van de bevoegd-heid wordt vastgelegd in een proces-verbaal of in een memorandum (art. 243 lid 1 Sv).	Geen informatie bekend	Verzamelde gegevens worden verstrekt op een gecertificeerde gegevens-drager. De nationale Veiligheidsdienst zal zorgen voor de integriteit van de verzamelde gegevens op de gegevensdrager (persoonlijke communi-catie, 23 januari 2023).	Geen informatie bekend	De nationale Veiligheidsdienst voert de bevoegdheid uit en is verantwoordelijk voor het waarborgen van de betrouwbaarheid, herleidbaarheid en integriteit van de verzamelde gegevens. Wat de Veiligheidsdienst precies doet, is staatsgeheim (persoonlijke communicatie, 23 januari 2023). Na de inzet moet het technisch hulpmiddel worden verwijderd (art. 233 lid 1 Sv).
Ierland	Nee	Niet aanwezig	Geen informatie bekend	Geen informatie bekend	Data moet ten minste drie jaar worden opgeslagen na het beëindigen van de bevoegdheid (art. 9 Surveillance Act).	Tenzij het tegendeel wordt bewezen, wordt veronder-steld dat technische hulp-middelen accurate informatie produceren (art. 14 lid 5 Surveillance Wet). Het is aan de verdediging om aan te tonen dat zich onrechtmatig-heden hebben voorgedaan.	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
						Tenzij een rechter anders bepaalt, geldt geen notificatieplicht (art. 15 Surveillance Wet).	
Italië	Nee	Niet aanwezig	Van alle activiteiten moet een verslag aanwezig zijn (art. 268/269 Sv).	Geen informatie bekend	Activiteiten vinden in beginsel plaats via de systemen van het Open-baar Ministerie, of als deze technisch te kort schieten via systemen van de recherche (naast het apparaat van de ver-dachte) (art. 268/269 Sv). Opnames moeten meteen naar de systemen van het Openbaar Ministerie worden verstuurd ter archivering (art. 268/269 Sv).	De verdachte heeft het recht de opnames terug te luisteren of 'met telematicamiddelen kennis te nemen van computer- of telematicacommunicatie-stromen' (art. 268/269 Sv).	Geen verdere informatie
Kroatië	Nee	Niet aanwezig	De politie brengt dagelijks een rapport uit over de uitvoering en documenteert technische handelingen. Dit rapport wordt naar de officier van justitie gestuurd (art. 337 lid 1 Sv).	De onderzoeksrechter kan op elk moment aan de officier van justitie vragen om een verslag van het verloop van de inzet. Ook kan de onderzoeksrechter informatie opvragen bij de politie. De politie maakt uiteindelijk een rapport op met daarin het begin- en het eindtijdstip van de inzet en de personen bij wie de bevoegdheid wordt toegepast (art. 337 lid 3 Sv).	De gegevens, het verslag en de documentatie worden verzegeld bewaard op het kantoor van de officier van justitie. Informatie die niet relevant is voor het onderzoek wordt eruit gehaald (art. 338 lid 2 Sv). De officier van justitie moet de verzegelde gegevens overhandigen aan de onderzoeksrechter en een deskundige assistent zal de relevante gegevens eruit halen (art. 338 lid 3 Sv). De verzameling van digitale gegevens dient met gecertificeerde technische hulpmiddelen te gebeuren, zodat gegevens niet veranderd worden (persoonlijke	Het Wetboek van Strafvordering bevat geen notificatieverplichting (Jurić & Roksandić, 2021, p. 397). Wel kan het bevel, na uitvoering ervan, op verzoek van de verdachte aan hem of haar worden overhandigd (art. 335 lid 5 Sv). Op verzoek van de verdediging dient inzage te worden gegeven in de gegevens. Na inzage kunnen de gegevens worden beluisterd of voorgelezen tijdens de rechtszaak (art. 338 lid 4 Sv).	Er zijn geen specifieke regels gericht op de toelaatbaarheid van onderschepte of opgeslagen elektronische communicatiegegevens. Algemene regels en principes met betrekking tot bewijs zijn geldig (Jurić & Roksandić, 2021, p. 406).

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
					communicatie, 31 oktober 2022).		
Letland	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Litouwen	Nee	Niet aanwezig	Gegevens die worden gebruikt voor waarheids-vinding moeten worden opgenomen in het dossier (persoonlijke communica-tie, 18 juli 2022). In het proces-verbaal dienen alleen voor het onderzoek relevante gegevens opgenomen te worden. Niet relevante gegevens en gegevens die op een gemeenschappe-lijke drager staan met daarop gegevens die voor de zaak relevant zijn, wod-en niet aan het dossier toegevoegd en worden, na een beslissing van de officier van justitie, ver-nietigd (art. 158 lid 8 Sv). Algemene waarborgen ten aanzien van elektronisch bewijs: aan bewijs dient de tijdsaanduiding te worden toegevoegd, zodat duidelijk is als wijzigingen plaats-vinden. Ook dient gebruik te worden gemaakt van elektronische handteke-ningen zodat duidelijk is wie het bewijs verzameld heeft. Verder dient gebruik te worden gemaakt van professionele tools. Wat professioneel is, is niet duidelijk geworden (persoonlijke communi-catie, 18 juli 2022).	Geen informatie bekend	Geen informatie bekend	Zodra de inzet van de bevoegdheid is beëindigd, dienen personen tegen wie de bevoegdheid is ingezet, zo snel mogelijk, maar zonder het succes van het opsporingsonderzoek te compromitteren, op de hoogte te worden gesteld dat de bevoegdheid is ingezet (art. 161 lid 1 Sv). Een verdachte heeft het recht om toegang te hebben tot gegevens uit het vooronder-zoek, met uitzondering van persoonsgegevens. Ook heeft de verdachte het recht om kopieën of uittreksels van het vooronderzoek te maken. Een officier van justitie heeft het recht de toegang tot (een deel van) die gegevens te weigeren. Tegen deze beslissing kan beroep worden aangetekend (art. 181 lid 1 Sv). Indien gegevens zijn verzameld en die gegevens worden niet bevestigd en er wordt geen gerechtelijk vooronderzoek ingesteld, maar een persoon heeft wel negatieve rechtsgevolgen ondervonden (als gevolg van de informatie die is verzameld), dan moeten op verzoek van deze persoon, deze gegevens aan de persoon worden overhandigd, met uitzondering van de in	In uitzonderlijke gevallen kunnen andere personen dan ambtenaren van het gerechtelijk vooronderzoek het onderzoek verrichten zoals bedoeld in artikel 158 Sv (art. 158 lid 6 Sv). Gedetailleerde informatie over de methoden en middelen die gebruikt worden voor het ver-zamelen van criminele inlichtingen, over de gebruikte tactieken, over de identiteit van undercovermedewerkers en over de samenstelling van het team worden niet prijsgegeven (art. 19 lid 7 Wci).

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
						de artikel 19 lid 7 van deze wet bedoelde gegevens (art. 5 lid 6 Wci). Tijdens de zitting kan de uitvoerder van het onderzoek worden opgeroepen als getuige (art. 158 paragraaf 7 Sv).	
Luxemburg	Nee	Niet aanwezig	Er moet een proces-verbaal worden opgesteld met daarin de handelingen die verricht zijn voor het (de-)installeren van de software en met de handelingen om computergegevens binnen te halen (art. 88-4 lid 2 Sv).	Geen informatie bekend	Er wordt een verzegelde kopie bewaard en overhandigd aan de rechter. Hij/zij kan de kopie door een technisch expert laten analyseren (art. 88-4 lid 3 Sv). Gegevens worden verwijderd na veroordeling of verstrijken van de termijn van vervolging (art. 88-4 lid 8 Sv).	De verdediging krijgt een kopie van de gegevens als de zaak ter zitting komt (art. 88-4 lid 5 Sv). Notificatie bij aanvang van de rechtszaak. De wet maakt geen melding van notificatie als er geen bruikbaar bewijs is gevonden (persoonlijke communicatie, 12 juli 2022 & 21 juli 2022).	Er moeten passende maatregelen worden genomen die de integriteit en vertrouwelijkheid van de gegevens verzekeren (art. 88-4 lid 3 Sv). Er is niet gespecificeerd wat deze maatregelen inhouden.
Noorwegen	Nee	Een kopie van een bevel wordt inclusief onderliggende documenten direct verstuurd naar de procureur-generaal (Regeling communicatiecontro-le, artikel 3). Daarnaast is er een controlecomité dat kijkt of bepaalde bevoegdheden, waaronder de gegevensuitlezing, plaatsvinden binnen het kader van de wet en de gegeven instructies. Ook kijkt dit comité of de inzet van dwangmiddelen beperkt is en of ze niet voor iets anders	De politie moet een over-zicht bijhouden waarin het volgende is opgenomen: naam van de instantie die de inzet uitvoert, het verzoek van het Openbaar Ministerie, het bevel, op welke geautomatiseerde werken de inzet gericht is en de start- en einddatum van de inzet (art. 7 lid 1 Verordeningen inzake toezicht op communicatie, ruimtebewaking en de gegevensuitlezing (*Forskrift om kommuni-kasjonskontroll, romavlytting og dataavlesing*) (hierna de Regeling communicatiecontrole) Daarnaast moet met	Geen informatie bekend	De politie moet zoveel mogelijk het risico proberen te voorkomen dat iemand onbevoegd toegang krijgt tot het geautomatiseerd werk of tot beschermde informatie, of dat iemand andere criminele feiten pleegt (art. 216p lid 2 Sv). De gegevens moeten op een behoorlijke en gepaste manier worden bewaard (art. 8 lid 1 Regeling communicatiecontro-le). Gegevens, overeenkomend met de beveiligingsinstructies, dienen te worden bewaard als dat nodig is in het kader van preventie en	De verdediging heeft het recht op toegang tot alle 'zaaksdocumenten' vastgesteld in artikel 242 en 264 Sv. Tijdens het onderzoek kan de toegang beperkt worden indien die het opsporingsonderzoek, andere onderzoeken of derde partijen in gevaar kunnen brengen (art. 242 Sv) (persoonlijke communicatie, 26 juni 2023). De term 'zaaksdocumenten' verwijst naar alle documenten die dienen als bewijs, zoals kaarten, foto's, tekeningen en geluidsopnames (art. 242 & 264 Sv en diverse uitspraken van het Hooggerechtshof, bijvoorbeeld HR-2017-274-U	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
		worden gebruikt dan voor redenen die in de wet genoemd worden (Regeling communicatiecontro-le, artikel 14). Het comité kan ook politiemensen en medewerkers van het Openbaar Ministerie interviewen, zonder beperkingen van vertrouwelijkheid. Elke inzet van de gegevensuitlezings-bevoegdheid, uitgevoerd door de politieveiligheidsdienst , wordt bekeken door de Noorse parlementaire commissie van toezicht op de inlichtingen en veiligheidsdiensten (‘*EOS-ytvalget*’ (EOS-wet)) (persoonlijke communicatie, 26 juni 2023).	betrekking tot de gegevensuitlezing ook een aantal andere onderwerpen worden geregistreerd. Het gaat onder meer om: het moment waarop apparatuur is geplaatst en verwijderd, of technische apparaten zoals hardware of software zijn gebruikt, of er fysiek is ingebroken, of de politie de beveiliging van het geautomatiseerd werk heeft gebroken of omzeild (art. 7 lid 2 Regeling communicatiecontrole).		opsporing. Indien specifiek bepaald, moeten gegevens op een meer zekere manier worden bewaard (art. 9 lid 2 Regeling communicatiecontrole). De korpschef zorgt voor afscherming van gegevens als deze volgens de regels in artikel 50 lid 3 van de Wet op het politieregister niet meer te bewaren zijn (art. 9 lid 3 Regeling communicatiecontrole).	en HR-2017-2145-U) (persoonlijke communicatie, 26 juni 2023).. In Noorwegen geldt na afloop van de inzet van de bevoegdheid een notificatieplicht (tenzij uitzonderingsregels gelden) (art. 216o lid 5 juncto art. 216j Sv).	
Oostenrijk	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Polen	Nee	Niet aanwezig	Alle uitgevoerde handelingen dienen te worden opgenomen in een proces-verbaal (art. 4, Ordonnantie op operationele controle uitgevoerd door de politie, hierna Ordonnantie).	Geen informatie bekend	Gegevens die niet relevant zijn voor de waarheidsvinding dienen onmiddellijk te worden verwijderd (art. 19 lid 17 Pw). Communicatiegegevens dienen herleidbaar te zijn naar de verzender en ontvanger (art. 6 Ordonnantie). Voor de opname van beeld, geluid en berichten wordt	Degene tegen wie de bevoegdheid is ingezet krijgt geen inzage in de gegevens die zijn verzameld (art. 19 lid 16 Pw).	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
					metadata gegeneerd en opgeslagen (art. 7 Ordonnantie). Opslagmedia bevatten een elektronisch certificaat op basis van de volgorde dat de opnames en kopieën zijn gemaakt van de gegevens (art. 8 Ordonnantie). Voor alle opgeslagen bestanden worden automatisch *checksums* gegenereerd (art. 9 Ordonnantie). Kopieën moeten in hetzelfde bestandsformaat worden gemaakt en de checksum moet consistent zijn met het originele bestand (art. 10 Ordonnantie). De opslag en overdacht van verkregen gegevens dienen te worden uitgevoerd op een manier die de vertrouwelijkheid van de gegevens waarborgt (art. 12 Ordonnantie).		
Portugal	Nee	Niet aanwezig	Politieambtenaren schrijven een verslag van de opnames die relevant zijn in het kader van het bewijs. Zij beschrijven de inhoud en waarom die relevant is voor het aan de dag brengen van de waarheid (art. 188 lid 1 Sv). Een rechter zal bevelen om technische materialen en	Elke twee weken overhandigt de politie het technisch materiaal, de opnames en de verslagen aan het Openbaar Ministerie (art. 188 lid 3 Sv). Binnen 48 uur moeten de gegevens aan de rechter worden gestuurd (art. 188 lid 4 Sv). Een deel van het verzamelde materiaal (technisch en voor de	Er kunnen kopieën van opnames worden gemaakt (art. 187 lid 8 Sv). Op bevel van de rechtbank worden technische materialen, in relatie tot gesprekken of communicatie die niet zijn getranscribeerd, in verzegelde enveloppen bewaard en vernietigd nadat een beslissing over	De verdediging en degene die de officier van justitie ondersteunen mogen toegang krijgen tot de onderschepte communicatie, maar alleen als het onderzoek openbaar is geworden (art. 188 lid 8 Sv) (persoonlijke communicatie, 12 juni 2023). De rechter kan de opnames beluisteren om te zien of deze correct getranscribeerd zijn en of dat andere	Artikel 19 Cybercrimewet: In de wet zijn geen regels opgenomen met betrekking tot de operationele aspecten of specifieke vereisten van de bevoegdheid. Er wordt niet verwezen naar technische regels die men in acht moet nemen bij het verkrijgen en opnemen van gegevens tijdens de inzet van de bevoegdheid. Ook

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
			verslagen die niet relevant zijn voor het onderzoek te vernietigen (art. 188 lid 6 Sv). De politie die de bevoegd-heid heeft uitgevoerd, zal uiterlijk 48 uur nadat de operatie beëindigd is een verslag schrijven (art. 3, lid 6 Wet 101/2001).	zaak niet relevant) dient vernietigd te worden (art. 188 lid 6 Sv). Verder kan de rechter de transcriptie van gegevens gelasten die een dwangbevel rechtvaardigen (art. 188 lid 7 Sv).	de zaak rechtskracht heeft gekregen (art. 188 lid 12 Sv). Informatie uit deze verzegelde envelop mag alleen worden gebruikt in geval van een buitengewoon beroep (art. 188 lid 13 Sv).	opnames moeten worden toegevoegd (art. 188 lid 10 Sv). De gerechtelijke autoriteit gelast slechts dat het in artikel 3, lid 6, bedoelde verslag aan het dossier wordt toegevoegd, indien zij dit uit een oogpunt van bewijsvoering absoluut onontbeerlijk acht (art. 4 lid 1 Wet 101/2001) (persoonlijke communicatie, 12 juni 2023).).	zijn er geen regels met betrekking tot het gebruik van malware, zoals het type malware, het installatieproces en het verzamelen van informatie (Verdelho, 2021, p. 1260 en 1261). Wet nr. 05/2022: De genoemde voorwaarden vastgelegd in artikel 188 Sv gelden ook voor dit artikel (art. 6 lid 3 Wet nr. 05/2022).
Roemenië	Nee	Niet aanwezig	In een proces-verbaal moeten alle uitgevoerde handelingen en bevin-dingen worden opgenomen (art. 143 lid 1 Sv).	Geen informatie bekend	Er moet een kopie van alle gegevens in een afgesloten envelop worden bewaard die door de rechtbank kan worden geraadpleegd (art. 143 lid 2 Sv). Voor het verkrijgen, versturen en ontvangen van de gegevens kan gewerkt worden met een elektronische hand-tekening, gebaseerd op een certificaat dat uitgevaardigd is door een geaccrediteerde service-provider die certificaten uitgeeft (art. 142 lid 1 Sv). Er is niet nader toegelicht wat dit precies inhoudt.	Geen informatie bekend	Geen verdere informatie
Slovenië	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Slowakije	Nee	Niet aanwezig	Wanneer de gegevens als bewijs worden gebruikt, moet een letterlijk transcript worden gemaakt. Dit moet worden gedaan door iemand van de politiedienst die de interceptie heeft uitgevoerd. Hierbij gaat het	Geen informatie bekend	De gegevens moeten in zijn geheel in 'geschikte elektronische dragers' worden opgeslagen (art. 115 lid 6 Sv). Voor de opslag van de gegevens wordt gebruik-gemaakt van hashing	Kopieën kunnen worden aangevraagd door de officier van justitie, de verdachte en/of de verdediging. De verdachte en de verdediging mogen ook zelf een transcript maken van de gegevens. De rechtbank beoordeelt de	Geen verdere informatie

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
			om de feiten die van belang zijn voor het strafproces. Ook moet informatie worden toegevoegd over de plaats, de tijd en de autoriteit die de opname heeft gemaakt en over de rechtmatigheid van de interceptie (art. 115 lid 6 Sv).		(persoonlijke communi-catie, 22 augustus 2022).	betrouwbaarheid van het transcript (art. 115 lid 6 Sv).	
Spanje	Nee	Niet aanwezig	In het dossier worden alle processen-verbaal opgenomen. Mocht de bevoegdheid geen bewijs opleveren, ook dan wordt er melding van gemaakt in het dossier (persoonlijke communicatie, 9 juni 2022).	De rechter moet erop toezien dat maatregelen zijn genomen zodat de gegevens in tact blijven (persoonlijke communicatie, 9 juni 2022). Indien de bevoegdheid langer wordt uitgevoerd dan de periode waarvoor toestemming is gegeven, kan de rechter-commissaris beslissen dat de verzamelde informatie niet meegenomen wordt (persoonlijke communicatie, 12 juni 2023).	Voor het maken en bewaren van kopieën op afstand moet de rechter apart toestemming geven (art. 588 lid 2 sub d Sv). Bij het maken van kopieën moeten voorzorgsmaat-regelen worden genomen om de integriteit en identiteit van de gegevens te waarborgen. De kopieën worden ondergebracht bij de griffier van het Hof (Eurojust). In de rechterlijke beslissing waar goedkeuring wordt gegeven voor de inzet van de bevoegdheid, moeten maatregelen worden beschreven voor 'het behoud van de integriteit' van gegevens, alsmede het ontoegankelijk maken of het verwijderen van de gegevens (art. 588 lid 2 sub e Sv; Eurojust; ministerio Fiscal, 2019 (Circulaire)).	De verdachte krijgt inzage in een kopie van de verzamelde gegevens. Wanneer de verdachte een kopie van de gegevens heeft, kan hij een derde partij vragen om deze kopie te onderzoeken (persoonlijke communicatie, 11 juli 2022).	In de rechterlijke beslissing waarin goedkeuring wordt gegeven voor de inzet van de bevoegdheid, moet worden vermeld op welke manier toegang zal worden verkregen tot de computer-gegevens, hoe deze zullen worden opgeslagen en welke software is gebruikt (art. 588 lid 2 sub b Sv). Bij software moet een indicatie worden gegeven (aan de verdediging als hij/zij daar om vraagt (persoonlijke communi-catie, 6 juni 2023)) van het programma. Hierbij kan worden gedacht aan de technische of commerciële naam of het type pro-gramma en de fabrikant. Wanneer programma's worden gebruikt die specifiek voor de politie zijn gecreëerd, hoeft alleen een indicatie te worden gegeven van het type programma (zoals een Trojan of een keylogger), en indien van toepassing de potentiële reikwijdte en de functies van het technisch hulpmiddel. Specifieke technische

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
							gegevens hoeven niet te worden gedeeld (ministerio Fiscal, 2019 (Circulaire)).
Tsjechië	Nee	Niet aanwezig	Indien een opname wordt gemaakt gedurende de surveillance en die opname wordt gebruikt als bewijs, dan moet een protocol worden opgesteld dat voldoet aan de voor-waarden in artikelen 55 en 55a Sv. Artikel 55 regelt onder andere dat een protocol wordt opgesteld van alle acties die worden uitgevoerd. In dat protocol is bijvoorbeeld aandacht voor: naam van instanties, plaats, tijd en onderwerp van de actie en een ver-klaring van de uitgevoerde acties (art. 55 lid 1 Sv). De rest van de inhoud van artikel 55 Sv heeft vooral betrekking op het afnemen van een verhoor. Om het verloop van een actie vast te leggen, kan een stenografisch verslag worden gemaakt dat samen met bijvoorbeeld geluid- en beeldopnames bij het verslag kan worden gevoegd (art. 55a lid 1 Sv). Indien naast het protocol audio- of video-opnames worden gemaakt, wordt dit in het protocol genoteerd. Het technisch opname-medium wordt bij het dossier gevoegd en er wordt aangegeven waar het medium is opgeslagen (art. 55a lid 2 Sv).	Geen informatie bekend	Geen wettelijk vastgelegde maatregelen. De politie zou hashing gebruiken en ervoor zorgen dat de authenticiteit van de gegevens technisch gegarandeerd is (per-soonlijke communicatie, 3 januari 2023). Indien uit de surveillance niets substantieels naar voren komt, dan worden de opnames volgens een voorgeschreven wijze vernietigd (art. 158d lid 8 Sv). Ook communicatie met een advocaat dient te worden vernietigd (art. 158d lid 1 Sv).	Als de politie haar onderzoek beëindigd heeft, en de resultaten zijn voldoende om een tenlastelegging in te kunnen vullen, dan krijgen de verdachte, de verdediging, en het slachtoffer de mogelijk-heid om binnen een redelijke termijn kennis te nemen van het dossier en verzoek-schriften in te dienen om het onderzoek aan te vullen. De politie kan de gevraagde aanvulling niet noodzakelijk achten en afwijzen (art. 166 lid 1 Sv).	Indien in de opnames informatie naar voren komt met betrekking tot andere strafbare feiten dan waarvoor het bevel is afgegeven, mogen die onder bepaalde voorwaarden als bewijs worden gebruikt, namelijk indien in die zaak een procedure inzake een opzettelijke criminele activiteit wordt gevoerd of indien de persoon wiens rechten en vrijheden werden aangetast, instemt (art. 158d lid 10 Sv). Telecommunicatieopera-toren zijn verplicht hun medewerking te verlenen aan de surveillance (art. 158d lid 9 Sv).

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
Verenigd Koninkrijk	Nee	Er is een Commissa-riaat voor Onder-zoeksbevoegdheden (‘*Investigatory Powers Commissioner’s Office*’, hierna IPCO). De IPCO is verant-woordelijk voor het toezicht op het gebruik van onder-zoeksbevoegd-heden, waaronder *equipment interference*: dat deze in overeenstemming met de wet en het algemeen belang worden ingezet (Eurojust). Klachten of geschillen met betrekking tot de inzet van onderzoeks-bevoegd-heden, waaronder *equipment interference*, kunnen worden behandeld door het onderzoeks-bevoegd-heden tribunaal (‘*Investigatory Powers Tribunal*’) (Eurojust).	Als gegevens als bewijs worden gebruikt in een strafzaak, moet worden aangetoond hoe het bewijsmateriaal is verzameld (voor de integriteit van het bewijs) (Eurojust; Home Office, 2018 (‘*Code of Practice*’)). In de ‘*code of practice*’ worden geen methoden gespecificeerd om de integriteit van bewijs-materiaal te behouden. In plaats daarvan concen-treert de Code zich op mogelijke conflicten met andere wetgeving, zoals de Wet Opsporingsbevoegdheden. De wet zegt dat gegevens die tijdens de overdracht worden onderschept, ontoelaatbaar zijn, niet als bewijs kunnen worden gebruikt en dat er niet naar kan worden verwezen (art. 56 WO).	Geen informatie bekend	In artikel 129 lid 2 (WO) staat beschreven dat de volgende onderwerpen moeten worden beperkt tot het minimum voor wat noodzakelijk is voor geautoriseerde doeleinden (deze doeleinden staan in lid 3 opgesomd): o Het aantal personen aan wie het verzamelde materiaal openbaar/ beschikbaar wordt gemaakt. - De mate waarin het verzamelde materiaal openbaar / beschikbaar wordt gemaakt. - De mate waarin het verzamelde materiaal wordt gekopieerd. - Het aantal kopieën. Kopieën van de verzamelde gegevens dienen op een veilige manier opgeslagen te worden (art. 129 lid 4 WO). Alle kopieën moeten zo snel mogelijk worden vernietigd als er geen gronden meer zijn om deze te bewaren (art. 129 lid 5 WO).	In het Verenigd Koninkrijk is de officier van justitie doorgaans verplicht om informatie vrij te geven op grond van de Wet Straf-vordering en opsporings-bevoegdheden 1996. Van de verdediging wordt verwacht dat zij een pleidooi voor de verdachte indient met een motivering voor specifieke soorten openbaarmaking. Als de partijen het niet eens zijn, kan de verdachte de recht-bank verzoeken om open-baarmaking. De rechtbank zal dan beslissen. Een van de gronden waarop de aanklager kan proberen om informatie achter te houden is immuni-teit van openbaar belang (IOO). Er zijn aanwijzingen dat de meeste "*equipment interference*"- activiteiten in het Verenigd Koninkrijk niet als bewijs worden geprodu-ceerd, maar worden achter-gehouden op grond van IOO. Zeer weinig hiervan hebben geleid tot de productie als bewijsmateriaal (Sommer, 2022, p. 3) (persoonlijke communicatie, 3 juni 2023).	Systemen gebruikt voor *equipment interference* zijn onderworpen aan interne onderzoeken. De gebruikte tools van de NCA zijn vertrouwelijk (Eurojust). In de '*Good Practice Guide for Digital Evidence*', opgesteld door de Association of Chief Police Officer's (ACPO) staan vier principes opgenomen met betrekking tot het forensisch onderzoek van digitale gegevens: 1 Geen actie mag worden ondernomen waardoor bewijsgegevens op een digitaal apparaat wijzigen. 2 De uitvoerende persoon moet bekwaam zijn en moet diens acties en de implicaties daarvan aan de rechtbank kunnen uitleggen. 3 Logging van alle verwerkingen van het digitale bewijs moet worden bijgehouden. Een onafhankelijke derde partij moet in staat zijn om deze processen te onderzoeken en moet tot dezelfde conclusie komen. 4 De onderzoeksleider is verantwoordelijkheid om ervoor te zorgen dat wordt voldaan aan de wet en aan deze principes. (Horsman, 2020; Sommer, 2022).

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
Verenigde Staten	Nee	Niet aanwezig	In principe wordt geen informatie prijsgegeven over de gebruikte methode (Gutheil et al., 2017). Bij rechtmatig hacken blijft 'de inventaris' beperkt tot het beschrijven van de fysieke opslag van de media die werden doorzocht en gekopieerd (Rule 41f lid 1b Federaal Sv).	Geen informatie bekend	De functionaris mag een kopie bewaren van in beslag genomen en gekopieerde elektronisch opgeslagen informatie (Rule 41f lid 1b Federaal Sv). Degene die het bevel uitvoert, moet het bevel, samen met de inventaris, terugzenden naar de rechter-commissaris. Dat kan worden gedaan met 'betrouwbare elektronische middelen' (Rule 41f lid 1d Federaal Sv). De rechter aan wie het bevel wordt geretourneerd, voegt bij een bevel een bewijs van teruggave toe, de inventaris en alle andere bijbehorende stukken, en overhandigt deze aan de griffie van het district waarin de inbeslag-name plaatsvond (Rule 41i Federaal Sv). Methoden hoeven niet te worden gespecificeerd. Veel van wat gebeurt op het gebied van hacken blijft buiten het zicht van de rechter. Bovendien blijven gerechtelijke bevelen vaak verzegeld (Gutheil et al., 2017).	De rechter dient op verzoek een kopie van 'de inventaris' te geven aan de verdachte en aan de aanvrager van het bevel (Rule 41f lid 1d). Gedurende een rechtszaak kan de rechter vragen om de code te openbaren. In één zaak onderdeel uitmakend van de 'Playpen investigation' weigerde de FBI dat en heeft een rechter om die reden het daarmee verzamelde bewijs verworpen (Gutheil et al., 2017).	Er is geen speciale wetgeving (anders dan de voorwaarden die gelden wanneer een bevel in het kader van het Vierde amendement moet worden gevraagd) waarin grond-rechten gewaarborgd worden die moeten worden gerespecteerd (Gutheil et al., 2017). Wel zou er een amendement bij Rule 41 Federaal Sv in de maak zijn dat ervoor moet zorgen dat de politie meer informatie moet geven over haar werkwijze. Dat zou betekenen dat er meer voorwaarden komen ten aanzien van transparantie (persoonlijke communi-catie, 27 juni 2022). Wat betreft bewijs, en eventuele bezwaren die daartegen gemaakt kunnen worden, gelden de algemene Federale bewijsregels (persoonlijke communicatie, 27 juni 2022). Voorbeelden van regels die mogelijk van toepassing zijn, zijn de inzet van een getuige-deskundige (Rule 702 Federale bewijsregels) en eisen met betrekking tot kennisgeving in een strafzaak door de openbaar aanklager (Rule 404 Federale bewijsregels).
Zweden	Nee	SIN voert toezicht uit op de uitvoering van de bevoegdheid. De rechtbank notificeert SIN als een inzet gaat	Geen informatie bekend	Geen informatie bekend	Geen informatie bekend	In beginsel dient een persoon zo spoedig mogelijk te worden genotificeerd, uiterlijk één maand nadat het vooronderzoek is afgerond	Er zijn interne politierichtlijnen over het gebruik van technische hulpmiddelen. Deze zijn vertrouwelijk en niet

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
		plaatsvinden. SIN kan in theorie iedere willekeurige zaak waarvan zij op de hoogte wordt gesteld aan haar toezicht onderwerpen (persoonlijke communicatie, 26 augustus 2022). Als SIN onregelmatigheden vaststelt, doet zij een uitspraak. De uitspraken van SIN zijn niet bindend, maar organisaties conformeren zich in beginsel aan de uitspraken van SIN (persoonlijke communicatie, 29 september 2022). Naast de rechtmatigheidstoets zijn er geen wettelijke criteria waarop het toezicht zich richt. Het toetsingskader is nog in ontwikkeling (persoonlijke communicatie, 26 augustus 2022).				(art. 31 hoofdstuk 27 Sv). Een melding kan achterwege blijven als het vooronderzoek betrekking heeft op de in lid 1 tot en met lid 7 beschreven misdrijven (art. 33 hoofdstuk 27 Sv) De verdachte krijgt tijdens een zitting inzage in het bewijsmateriaal dat er tegen hem wordt gebruikt. De verdachte kan, onderbouwd, verzoeken om meer gegevens in te zien (persoonlijke communicatie, 9 november 2022). De officier van justitie kan de betrokken politieambtenaar als getuige oproepen om toe te lichten welke handelingen zijn verricht en op welke wijze de kwaliteit van de gegevens is gewaarborgd (persoonlijke communicatie, 2022).	openbaar beschikbaar. De politie maakt waar mogelijk gebruik van gestandaardiseerde of gecertificeerde software (bijvoorbeeld door de politie in het buitenland) (persoonlijke communicatie, 6 juli 2022).
Zwitserland	Nee	Niet aanwezig	Het versturen van gegevens van het geautomatiseerd werk van de verdachte naar de politie en het Openbaar Ministerie (‘*Strafverfolgungsbehörde*’) moet veilig verlopen (art. 269quater paragraaf 2 Sv). Speciale software moet worden gebruikt die de surveillance ‘onveranderlijk	Geen informatie bekend	Opnames van een geautoriseerde surveillance operatie die niet nodig zijn voor de strafzaak, worden apart van de processtukken bewaard en onmiddellijk na beëindiging van de procedure vernietigd (art. 276 paragraaf 1 Sv).	De officier van justitie brengt, op zijn laatst nadat het vooronderzoek is beëindigd, een verdachte op de hoogte van de inzet van de bevoegdheid (art. 279 lid 1 Sv). Notificatie kan achterwege worden gelaten (art. 279 lid 2a en 2b Sv).	Een strafrechtelijke autoriteit moet ervoor zorgen dat de broncode gecontroleerd kan worden om te kunnen verifiëren of de software alleen de wettelijk toegestane functies bevat (art. 269quater paragraaf 3 Sv) Politie en OM beschrijven een gedetailleerd proces voor het gebruik en de

Land	Keuring tech-nische hulp-midde-len	Controlerende instantie	Documenteren handelingen & logging	Rechterlijk toezicht	Opslag gegevens	Zitting & inzagerecht	Overig
			en zonder onderbreking' opneemt. De opname maakt onderdeel uit van het dossier (art. 269quater paragraaf 1 Sv). De politie stelt met behulp van processen-verbaal relevante feiten vast, aanwijzingen van de officier van justitie of eigen vaststellingen (art. 306 Sv lid 1). In het verslag aan de officier van justitie besteedt de politie onder andere aandacht aan dat er gegevens zijn opge-haald, dat die opgeslagen zijn en dat ze zijn gehasht. Over de exacte werkwijze van GovWare wordt geen informatie openbaar gemaakt (persoonlijke communicatie, 18 januari 2023). Logging dient ervoor te zorgen dat alle gevolgde stappen traceerbaar zijn (EJPD, 2023). In de praktijk zou het niet gaan om technische logging, maar om het laten zien welk soort gegevens binnengehaald is (persoonlijke communi-catie, 18 januari 2023).		Maatregelen worden genomen om gegevens veilig te kunnen versturen, bijvoorbeeld hashing en het werken met forensische containers (persoonlijke communi-catie, 18 januari 2023).		werking van GovWare. Daarin wordt onder andere aandacht besteed aan de autorisaties (EJPD, 2023).

Bijlage 4 Uitgebreide landbeschrijving Nederland[255]

Wettelijke regeling
Met de Wet computercriminaliteit III (hierna Wet CCIII) heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering (art. 126nba, 126uba en 126zpa Sv).[256] De nieuwe bevoegdheid maakt het mogelijk dat opsporingsambtenaren, 'onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk [kunnen] binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten'. Na het binnendringen van een geautomatiseerd werk mag de politie een aantal onderzoekshandelingen verrichten, namelijk:

- de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
- de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie (art. 126l Sv) of het aftappen en opnemen van communicatie (art. 126m Sv);
- de uitvoering van een bevel tot stelselmatige observatie (art. 126g Sv);
- de vastlegging van gegevens die in het geautomatiseerd werk zijn of worden opgeslagen;
- de ontoegankelijkmaking van gegevens, bijvoorbeeld het onschadelijk maken van een botnet.[257]

De Wet CCIII kent verder een aantal grondslagen om bij of krachtens Algemene Maatregel van Bestuur regels te stellen met betrekking tot de uitvoering van de hackbevoegdheid. Dat is bijvoorbeeld gebeurd in het Besluit onderzoek in een geautomatiseerd werk (hierna Besluit).

Bevoegde autoriteiten
Binnen het Openbaar Ministerie is vanuit verschillende niveaus betrokkenheid bij de controle op de inzet van de bevoegdheid, zowel voorafgaand aan de inzet als tijdens de inzet. Een deel van die betrokkenheid vloeit logisch voort uit artikel 126nba, lid 1 Sv. De officier van justitie stelt een vordering tot machtiging op voor de rechter-commissaris en later, als de machtiging wordt verleend, een bevel voor de politie. Voorafgaand hieraan is de landelijk officier van justitie betrokken die deze bevoegdheid in zijn of haar portefeuille heeft (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 19). Deze officier stuurt onder andere het politieteam aan dat uitvoering geeft aan de hackbevoegdheid. Voordat de officier van justitie definitief een vordering tot machtiging doet, wordt de voorgenomen inzet voorgelegd aan de Centrale Toetsingscommissie (CTC).[258] De CTC legt haar advies vervolgens voor aan het College van

[255] Dit hoofdstuk is gebaseerd op en grotendeels overgenomen uit het rapport over de uitvoering van de hackbevoegdheid in Nederland (Van Uden & Van den Eeden, 2022).
[256] Artikelen 126nba, 126uba en 126zpa Sv.
[257] 'Een botnet is een netwerk van aan het internet verbonden gecompromitteerde (computer-)systemen, die op afstand kunnen worden aangestuurd (Van der Waagen & Bernaards, 2018, p. 59)'. Een dergelijk netwerk kan ervoor zorgen dat kwaadaardige software wordt verspreid (Van der Waagen & Bernaards, 2018, p. 60), waardoor bijvoorbeeld toetsaanslagen van de computergebruiker worden vastgelegd (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 22).
[258] De CTC is een intern adviesorgaan binnen het Openbaar Ministerie. Zij toetst de inzet aan wet- en regelgeving, jurisprudentie, proportionaliteit, subsidiariteit en de mogelijke afbreukrisico's. Daarnaast overweegt de CTC de effectiviteit van de bevoegdheid en het afbreukrisico tegen het belang van de hantering van de bevoegdheid in een concreet geval.

Procureurs-Generaal,[259] die een definitieve beslissing neemt. Daarbij wordt onder andere het rechtmatigheidscriterium meegenomen.[260]

Nadat de procureur-generaal akkoord is met een mogelijke inzet van de hackbevoegdheid, dient de officier van justitie een vordering tot machtiging in bij de rechter-commissaris. Een rechter-commissaris beoordeelt mogelijke inzetten indien deze een inbreuk op de privacy opleveren en wanneer er een risico bestaat voor de beheersbaarheid en de integriteit van de opsporing.

De daadwerkelijke uitvoering van de hackbevoegdheid ligt in handen van speciaal daartoe aangewezen opsporingsambtenaren (Digit-politie) die onderdeel uitmaken van een specialistisch team van de Landelijke Eenheid van de Nationale Politie. Dit team is op dit moment het enige politieteam in Nederland dat de hackbevoegdheid uitvoert. De resultaten van de hack worden overgedragen aan het tactisch onderzoeksteam dat het opsporingsonderzoek uitvoert.[261]

Tegen wie
Een inzet van de bevoegdheid dient gericht plaats te vinden. Dat betekent dat mag worden binnengedrongen in een geautomatiseerd werk dat bij de verdachte(-n) in gebruik is.[262] Een bevel kan betrekking hebben op meerdere geautomatiseerde werken, mits de verdachte het geautomatiseerde werk gebruikt en dat het binnendringen noodzakelijk wordt geacht voor de opsporing van strafbare feiten.[263]

Gevallen
De bevoegdheid mag ten eerste worden gebruikt voor de opsporing van misdrijven als bedoeld in artikel 67 lid 1 Sv, zogenoemde voorlopige hechtenis-feiten ('VH-feiten') en voor misdrijven die een ernstige inbreuk op de rechtsorde opleveren.[264] Ten tweede is de bevoegdheid bedoeld voor een onderzoek naar personen ten aanzien van wie een redelijk vermoeden bestaat dat zij zich bezighouden met het beramen en/of plegen van misdrijven in georganiseerd verband.[265] Ten derde kan de bevoegdheid worden ingezet wanneer er aanwijzingen zijn voor een terroristisch misdrijf.[266] Afhankelijk van het opsporingsdoel dat opsporingsinstanties voor ogen hebben, gelden een aanvullend vierde en vijfde criterium. Wanneer opsporingsinstanties gegevens veilig willen stellen[267] en/of ontoegankelijk willen maken,[268] moet sprake zijn van een misdrijf waarvoor volgens de wettelijke omschrijving een gevangenisstraf van acht jaar of meer kan worden opgelegd. Ook zijn deze opsporingshandelingen toegestaan in opsporingsonderzoeken naar misdrijven die bij Algemene Maatregel van Bestuur zijn aangewezen. Het gaat dan om misdrijven waarvoor geen gevangenisstraf van acht jaar of meer geldt, maar die met een geautomatiseerd werk worden gepleegd en die een geautomatiseerd werk als doel hebben.[269] Ook betreft het, aldus het Besluit, ernstige commune misdrijven die steeds vaker met behulp van een geautomatiseerd werk worden gepleegd. Voor al deze misdrijven zou gelden dat er vaak geen ander

[259] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 38.
[260] *Kamerstukken I* 2016/17, 34 372, D.
[261] Besluit onderzoek in een geautomatiseerd werk, p. 14.
[262] Artikel 126nba, lid 1 Sv.
[263] *Kamerstukken II* 2015/16, 34 372, nr. 6, p. 13.
[264] Artikel 126nba Sv.
[265] Artikel 126uba Sv.
[266] Artikel 126zpa Sv.
[267] Artikel 126nba, lid 1, sub D Sv.
[268] Artikel 126nba, lid 1 sub E Sv.
[269] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2. Een voorbeeld van een misdrijf is het opzettelijk en wederrechtelijk voor zichzelf of voor een ander overnemen van niet openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk (art. 138c Sr).

aanknopingspunt is voor de opsporing dan het geautomatiseerd werk waarmee het misdrijf wordt gepleegd.[270] Bovendien is er een duidelijk maatschappelijk belang bij de beëindiging van de strafbare situatie en de vervolging van de daders.[271]

Termijn
De bevoegdheid mag voor een periode van maximaal vier weken worden toegepast. Deze periode kan steeds met een periode van ten hoogste vier weken worden verlengd.[272] Er geldt géén maximale periode dat de bevoegdheid mag worden ingezet. Ook is géén maximaal aantal verlengingen geregeld. Op het moment dat Digit-politie het doel van het onderzoek in een geautomatiseerd werk heeft bereikt, of de geldigheidsduur van het bevel is verlopen, zal de politie het onderzoek beëindigen.

Formaliteiten
Een bevel voor een inzet van de hackbevoegdheid dient schriftelijk te worden gegeven en in het bevel moeten in elk geval de volgende onderwerpen worden vermeld:[273]
- het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
- zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerd werk kan worden geïdentificeerd en, indien bekend, een aanduiding dat de gegevens niet in Nederland zijn opgeslagen;
- de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in artikel 126nba, lid 1 Sv zijn vervuld;
- een aanduiding van de aard en functionaliteit van het technisch hulpmiddel, zoals bedoeld in artikel 126nba, lid 1 Sv, dat wordt gebruikt voor de uitvoering van het bevel;
- het onderdeel of de onderdelen, genoemd in artikel 126nba, lid 1 Sv, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft,[274] een duidelijke omschrijving van de te verrichten handelingen;
- ten aanzien van welk deel van het geautomatiseerd werk en ten aanzien van welke categorie van gegevens aan het bevel uitvoering wordt gegeven;
- het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;
- in het geval het een bevel, bedoeld in artikel 126nba, lid 1c Sv[275] betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

Een bevel kan alleen worden gegeven na een schriftelijke machtiging door de rechter-commissaris, nadat de officier van justitie een vordering tot machtiging heeft ingediend. In de machtiging dienen alle onderdelen van het bevel te worden vermeld en de periode dat de machtiging van kracht is.[276] Indien sprake is van dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven. Wel dienen de officier van justitie en de rechter-commissaris hun beslissing binnen drie dagen op schrift te stellen.[277]

[270] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 11.
[271] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 11.
[272] Artikel 126nba, lid 3 Sv; *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54.
[273] Artikel 126nba, lid 2a t/m h Sv.
[274] A = de vaststelling van bepaalde kenmerken van het geautomatiseerd werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan. D = de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en E = de ontoegankelijkmaking van gegevens.
[275] De uitvoering van een bevel tot stelselmatige observatie (art. 126g Sv).
[276] Artikel 126nba, lid 4 Sv.
[277] Artikel 126nba, lid 5 Sv.

In artikel 126nba, lid 8 Sv is vastgelegd dat bij of krachtens Algemene Maatregel van Bestuur regels worden gesteld omtrent (a) de autorisatie en deskundigheid van de opsporingsambtenaren die kunnen worden belast met het binnendringen en het onderzoek zoals bedoeld in artikel 126nba, lid 1 Sv, en de samenwerking met andere opsporingsambtenaren; en (b) de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, zoals bedoeld in artikel 126nba, lid 1 Sv. In artikel 126nba, lid 9 Sv staat tot slot beschreven dat regels kunnen worden gesteld over de toepassing van de bevoegdheid, zoals bedoeld in artikel 126nba, lid 1 Sv in de gevallen waarin niet bekend is waar de gegevens zijn opgeslagen. Hoe gehandeld dient te worden wanneer een geautomatiseerd werk zich in het buitenland bevindt, is uiteindelijk beschreven in de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid.[278]

Technische hulpmiddelen

Voor het verrichten van onderzoekshandelingen kan een technisch hulpmiddel worden gebruikt. Een technisch hulpmiddel is een 'softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2). Het gebruik van een technisch hulpmiddel is niet 'strikt noodzakelijk'. Soms zullen handelingen 'ad hoc en handmatig'[279] worden verricht.[280]

Een technisch hulpmiddel kent één of meerdere functionaliteiten, zoals het maken van screenshots, het opnemen van geluid, het vastleggen van toetsaanslagen en/of het doorzoeken van bestandsmappen om vervolgens gegevens daaruit vast te leggen. De benodigde functionaliteiten dienen in het bevel van de officier van justitie te worden vastgelegd en gedurende het onderzoek moet het technisch hulpmiddel zodanig zijn ingericht dat alleen de functionaliteiten zoals beschreven in het bevel daadwerkelijk kunnen worden gebruikt.[281] Gegevens die verzameld worden, worden gestuurd naar de technische infrastructuur[282] van de politie.[283] Een technische infrastructuur is de opslaglocatie voor gegevens die tijdens de uitvoering van een bevel worden vastgelegd.[284]

Waarborgen

Eisen technisch hulpmiddel

In het Besluit worden diverse eisen gesteld aan een technisch hulpmiddel. Een deel van deze eisen is gericht op het bevorderen van de betrouwbaarheid, integriteit en herleidbaarheid van gegevens. Op basis van het Besluit kunnen deze als volgt worden gedefinieerd.[285] Betrouwbaarheid betekent dat de gegevens die op een geautomatiseerd werk staan en gegevens die door een technisch hulpmiddel worden geregistreerd exact met elkaar overeen moeten komen. Integriteit houdt in dat de werking van een technisch hulpmiddel niet wijzigt en dat de geregistreerde gegevens niet wijzigen. Integriteit betekent ook dat onbevoegden geen toegang hebben tot de gegevens. Tot

[278] Staatscourant, 26 februari 2019, nr. 10277.
[279] Indien geen technisch hulpmiddel wordt gebruikt door Digit, is sprake van een handmatige inzet (Van Uden & Van den Eeden, 2022, p. 9). Vanwege de leesbaarheid van dit hoofdstuk, wordt geen aandacht besteed aan manieren om onderzoekshandelingen ad hoc en handmatig te verrichten.
[280] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16.
[281] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 37; artikel 8 Bogw.
[282] Met een technische infrastructuur wordt een 'technische voorziening van een technisch team (Digit-politie) bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2).
[283] Artikel 13, lid 1 Bogw.
[284] Besluit onderzoek in een geautomatiseerd werk, p. 33.
[285] De definities zijn afgeleid van het Besluit, omdat er geen specifieke definities zijn opgenomen in het Besluit.

slot houdt herleidbaarheid in dat duidelijk is dat de geregistreerde gegevens afkomstig zijn van het gebruikte technisch hulpmiddel.
In het Besluit is vastgelegd dat een technisch hulpmiddel in elk geval aan de volgende eisen dient te voldoen:

- Een technisch hulpmiddel moet zodanig zijn ingericht dat de werking ervan kan worden beperkt tot de functionaliteit/functionaliteiten die in het bevel genoemd staat/staan (gerichte werking).[286]
- Een technisch hulpmiddel detecteert en registreert alleen gegevens ten behoeve van de in het bevel genoemde functionaliteit/functionaliteiten (gerichte detectie en registratie).[287]
- Een technisch hulpmiddel dat beschikt over één of meerdere functionaliteiten ten behoeve van het opnemen van telecommunicatie detecteert en registreert alleen de communicatie die plaatsvindt door gebruik te maken van één of meerdere identificerende kenmerken van het geautomatiseerd werk van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft (gerichte detectie en registratie).[288]
- Een technisch hulpmiddel registreert gegevens op zo'n manier dat de inhoud van de geregistreerde gegevens identiek is aan de inhoud van de gedetecteerde gegevens (betrouwbaarheid en integriteit).[289]
- Een technisch hulpmiddel is beveiligd tegen wijziging van de werking ervan, tegen wijziging van de geregistreerde gegevens en tegen kennisneming van de geregistreerde gegevens door onbevoegden (betrouwbaarheid en integriteit).[290] Hierbij gaat het om beveiligingsmaatregelen die de beïnvloeding van een technisch hulpmiddel van buitenaf 'naar de stand van de techniek' zo goed mogelijk tegengaan. Denk daarbij aan authenticatiemaatregelen voor de communicatie met het technisch hulpmiddel of versleuteling van gegevens middels een digitale handtekening. Dat laatste zorgt ervoor dat de gegevens die het technisch hulpmiddel geregistreerd heeft, onleesbaar en ontoegankelijk zijn.[291]
- Een technisch hulpmiddel voorziet de geregistreerde gegevens van een uniek gegeven (herleidbaarheid).[292] Uit dit gegeven dient de relatie met het geplaatste technische hulpmiddel te blijken. Een voorbeeld van een uniek gegeven is een code die bij het plaatsen van het technisch hulpmiddel is toegevoegd.[293]
- Een technisch hulpmiddel voorziet de geregistreerde gegevens van de datum en tijd waarop de registratie plaatsvindt (datum en tijd).[294] Hiermee wordt bedoeld dat er zekerheid bestaat over de datum en over het tijdstip van de gegevensregistratie door een technisch hulpmiddel zodra een technisch hulpmiddel gegevens registreert.[295]
- Een technisch hulpmiddel transporteert de geregistreerde gegevens automatisch naar de technische infrastructuur van de politie (transport).[296]
- Een technisch hulpmiddel beveiligt de geregistreerde gegevens tijdens het transport naar een technische infrastructuur tegen wijziging van de geregistreerde gegevens en kennisneming van de geregistreerde gegevens door onbevoegden (transport).[297]

Verder is in artikel 22 van het Besluit geregeld dat de korpschef van de politie één of meer ambtenaren aanwijst die de centrale registratie van de toegang tot de technische

[286] Artikel 8 Bogw.
[287] Artikel 9, lid 1 Bogw.
[288] Artikel 9, lid 2 Bogw.
[289] Artikel 10, lid 1 Bogw.
[290] Artikel 10, lid 2 Bogw.
[291] Besluit onderzoek in een geautomatiseerd werk, p. 39.
[292] Artikel 11 Bogw.
[293] Besluit onderzoek in een geautomatiseerd werk, p. 39.
[294] Artikel 12 Bogw.
[295] Besluit onderzoek in een geautomatiseerd werk, p. 39.
[296] Artikel 13, lid 1 Bogw.
[297] Artikel 13, lid 2 Bogw.

hulpmiddelen voor hun rekening nemen. Ook is in dat artikel geregeld hoe de overdracht van het technisch hulpmiddel aan degene die de bevoegdheid daadwerkelijk gaat uitvoeren, plaatsvindt en wat geregistreerd moet worden ten aanzien van het technisch hulpmiddel dat overgedragen wordt.
De verzamelde gegevens moeten in principe direct getransporteerd worden naar de technische infrastructuur van Digit-politie.[298] Alleen ambtenaren die door de korpschef zijn aangewezen hebben toegang tot deze infrastructuur.[299] Bij het vastleggen van gegevens dienen maatregelen genomen te worden om wijziging van de vastgelegde gegevens of kennisneming van de vastgelegde gegevens door onbevoegden te voorkomen. Ook dient achteraf vastgesteld te kunnen worden of wijziging of kennisneming hiervan heeft plaatsgevonden.[300]

Na beëindiging van een inzet, wordt het technisch hulpmiddel voor zover als mogelijk verwijderd, zodat de politie geen gegevens meer kan ontvangen.[301] Er kunnen zich situaties voordoen waarin besloten wordt om een technisch hulpmiddel niet te verwijderen of de aangebrachte wijzigingen aan het geautomatiseerd werk niet ongedaan te maken. Aan een dergelijke beslissing dienen zwaarwegende belangen ten grondslag te liggen. Daarbij kan gedacht worden aan de reële kans dat verwijdering een flink risico oplevert voor het geautomatiseerd werk waarop het technisch hulpmiddel geplaatst is. Mocht een technisch hulpmiddel niet volledig verwijderd worden, dan zorgt Digit-politie ervoor dat de politie geen gegevens meer kan ontvangen van het betreffende geautomatiseerd werk.[302] Bovendien zal de officier van justitie de beheerder van het geautomatiseerd werk op de hoogte stellen en informatie verstrekken zodat (sporen van) de software verwijderd kunnen worden.[303] Van de verwijdering van het technisch hulpmiddel of van het feit dat het transport van gegevens stop is gezet, dient een proces-verbaal opgemaakt te worden.[304] Op basis van logging zou kunnen worden gecontroleerd of het ontvangen van gegevens op de technische infrastructuur daadwerkelijk gestopt is. De Inspectie neemt het verwijderproces mee in haar toezicht.[305] In de paragraaf 'extern toezicht' wordt een toelichting gegevens op de rol van deze Inspectie.
De vastgelegde gegevens worden uiteindelijk verstrekt aan een opsporingsambtenaar die belast is met het opsporingsonderzoek.[306] Indien het voor het uitvoeren van het bevel of voor het opsporingsonderzoek nodig is om een selectie te maken uit de op een technische infrastructuur vastgelegde gegevens, voert een opsporingsambtenaar van Digit-politie een bewerking uit. Daarbij maakt hij/zij gebruik van een kopie van de op grond van artikel 27 van het Besluit vastgelegde gegevens. Bij het selecteren van gegevens legt een opsporingsambtenaar van Digit-politie de bewerkingen, die hebben plaatsgevonden met betrekking tot de kopie van de vastgelegde gegevens, vast in een proces-verbaal. Dit proces-verbaal wordt aan de officier van justitie gezonden.[307]

Keuring technisch hulpmiddel
Een technisch hulpmiddel dient, voorafgaand aan het gebruik ervan, gekeurd te worden.[308] Indien een technisch hulpmiddel goedgekeurd wordt, kan worden

[298] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40; artikel 27, lid 1 Bogw.
[299] *Kamerstukken I* 2016/17, 34 372, D, p. 41 en art. 28, lid 2 Bogw.
[300] Artikel 28, lid 3 Bogw.
[301] Artikel 126nba, lid 6 Sv; *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36.
[302] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36; artikel 26, lid 1 Bogw.
[303] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36-37; artikel 26, lid 2 Bogw.
[304] Artikel 26, lid 3 Bogw.
[305] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 47.
[306] Artikel 29, lid 1 Bogw.
[307] Artikel 29, lid 3 Bogw.
[308] Artikel 14 Bogw.

aangenomen dat aan de wettelijke eisen met betrekking tot de betrouwbaarheid, integriteit en herleidbaarheid van gegevens is voldaan.[309] Een keuringsdienst neemt de keuring voor haar rekening.[310]

De wijze waarop een keuring plaatsvindt wordt omschreven in een keuringsprotocol,[311] dat niet openbaar is. Daarin worden tevens criteria opgenomen die tijdens de keuring worden gebruikt. De keuringsdienst en het Openbaar Ministerie zijn samen verantwoordelijk voor het opstellen van een protocol dat de Minister van Justitie en Veiligheid voorafgaand aan het gebruik ervan goed moet keuren.[312]
In het Besluit zijn, zoals gezegd, regels geformuleerd ten aanzien van de technische eisen die gesteld worden aan een technisch hulpmiddel en de keuring ervan.[313] Bij de keuring dient gekeken te worden naar alle onderdelen van het hulpmiddel die belangrijk zijn voor de 'detectie, registratie en het transport van de gegevens'.[314] De technische infrastructuur van Digit is géén onderwerp van keuring.[315] Het is verder de bedoeling dat de keuring 'proefondervindelijk' plaatsvindt.[316] De verwachting is dat deze keuring enkele maanden in beslag kan nemen, zeker wanneer de gebruikte software nog moet worden aangepast om definitief goedgekeurd te worden.[317] Op het moment dat de keuring is afgerond, dient de keuringsdienst haar bevindingen vast te leggen in een keuringsrapport[318] inclusief een uniek keuringsnummer.[319] Het veronderstelde voordeel van zo'n uniek nummer is dat in het opsporingsdossier verder niets vermeld hoeft te worden over de precieze werking van het hulpmiddel. Daardoor is de kans kleiner dat opsporingsbelangen worden geschonden. Bovendien hebben rechters en advocaten de garantie dat het ingezette hulpmiddel voldoet aan alle wettelijke eisen.[320]

Een technisch hulpmiddel wordt alleen goedgekeurd als aan *alle* gestelde eisen in de artikelen 8 t/m 13 van het Besluit wordt voldaan.[321] Soms zal dat onmogelijk zijn. In dat geval moeten vervangende waarborgen worden gerealiseerd.[322] Indien sprake is van een inzet zonder technisch hulpmiddel, moeten procedurele waarborgen worden getroffen,[323] bijvoorbeeld het audiovisueel vastleggen van onderzoekshandelingen.[324]
De geldigheidsduur van het keuringsrapport zal worden vermeld in het rapport.[325]
Indien binnen die periode de werking van een technisch hulpmiddel of een onderdeel hiervan op zo'n manier wijzigt dat niet meer aan de gestelde technische eisen kan worden voldaan, moet een herkeuring worden uitgevoerd.[326] De Inspectie houdt toezicht op de wijze waarop de keuringsprocedure wordt nageleefd.[327]
In principe dient gebruik te worden gemaakt van een vooraf gekeurd en goed bevonden technisch hulpmiddel.[328] Keuring achteraf behoort ook tot de

[309] Besluit onderzoek in een geautomatiseerd werk, p. 19.
[310] Artikel 14, lid 1 Bogw.
[311] Artikel 17, lid 1 Bogw.
[312] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42.
[313] Artikel 8 t/m 20 Bogw.
[314] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42.
[315] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42.
[316] Besluit onderzoek in een geautomatiseerd werk, 2018.
[317] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40.
[318] Artikel 18 lid 2 Bogw.
[319] Artikel 18 lid 3b Bogw.
[320] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43.
[321] Artikel 14, lid 2 Bogw.
[322] Artikel 18, lid 3e Bogw.
[323] Artikel 21 lid 5 Bogw.
[324] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 45.
[325] Artikel 18, lid 3g Bogw.
[326] Artikel 14, lid 3 Bogw.
[327] Besluit onderzoek in geautomatiseerd werk, 2018, p. 43.
[328] Besluit onderzoek geautomatiseerd werk, p. 21.

mogelijkheden.[329] Verder kan het zijn dat de aard van een technisch hulpmiddel zich verzet tegen een keuring.[330] Als dat laatste aan de orde is, moet de officier van justitie in de processtukken opmerken dat afgezien is van keuring. Tevens dient hij of zij op te nemen welke aanvullende waarborgen zijn getroffen[331] om de 'betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te garanderen'.[332]

Logging

Logging, ofwel het continu vastleggen van onderzoekshandelingen die verricht worden, is (ook) een manier om de betrouwbaarheid, integriteit en herleidbaarheid van bewijs te waarborgen. Het Besluit maakt onderscheid tussen vier vormen van logging:[333]

1 Inzetlogging: deze vorm van logging heeft betrekking op het automatisch vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar van Digit-politie. Ook betreft deze vorm van logging de communicatie tussen de technische infrastructuur en het geautomatiseerd werk, de gebruikte scripts en softwareversies en het journaal dat de opsporingsambtenaar bijhoudt. In principe is het de bedoeling dat alles automatisch wordt vastgelegd. Indien dat niet mogelijk blijkt, dan moet binnen de politieorganisatie worden vastgelegd dat de logging handmatig gebeurt.
2 Bewijslogging: dit is een onderdeel van de zojuist besproken inzetlogging. Bewijslogging gaat over het vastleggen van gegevens gedurende de onderzoeksfase, al dan niet met behulp van een technisch hulpmiddel. Deze gegevens kunnen gebruikt worden in een strafzaak.
3 Systeemlogging: deze vorm heeft betrekking op de logging die reeds plaatsvindt door (alle) gebruikte systemen en die op centraal niveau wordt verzameld en vastgelegd. Systeemlogging moet ertoe bijdragen dat problemen met betrekking tot de betrouwbaarheid, integriteit en de beschikbaarheid van de technische infrastructuur worden gesignaleerd en opgelost.
4 Authenticatie- en autorisatielogging: een subonderdeel van systeemlogging dat betrekking heeft op de toegang tot een technisch hulpmiddel.

Extern toezicht

Inspectie Justitie en Veiligheid

Naast keuringen door de Keuringsdienst, houdt de Inspectie 'systeemtoezicht' op de uitvoering van de bevoegdheid.[334,335] De Inspectie ziet toe op de wijze waarop de politie haar taak uitvoert.[336] Vanuit die rol houdt zij (ook) toezicht op 'het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk'.[337] De Inspectie kan haar toezicht zelf vormgeven en is niet afhankelijk van meldingen die van buitenaf komen.[338] In haar toezicht neemt de Inspectie diverse onderwerpen mee.[339] Zo dient zij aandacht te besteden aan de autorisatie van de betrokken opsporingsambtenaren en hun kennis en expertise, de inzet van technische hulpmiddelen (inclusief de vraag of gegevens op een zorgvuldige

[329] Artikel 15, lid 1 Bogw.
[330] Artikel 21, lid 4 Bogw.
[331] Artikel 21, lid 4 Bogw.
[332] Besluit onderzoek geautomatiseerd werk, p. 21.
[333] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 17-18.
[334] *Kamerstukken II*, Handelingen 13 december 2016, nr. 34.
[335] Dit systeemtoezicht is er gekomen, mede omdat de verwachting was van de Raad van State dat rechters niet altijd goed in staat zullen zijn om de wijze waarop het onderzoek heeft plaatsgevonden goed te kunnen beoordelen. Bovendien zullen niet alle zaken waarin de hackbevoegdheid is ingezet, voorgelegd worden aan een rechter (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 8).
[336] *Kamerstukken II* 2016/17, 34 372, nr. 6.
[337] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23; artikel 126nba, lid 7 Sv.
[338] *Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 47.
[339] Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23-24.

manier en binnen de bestaande kaders worden verwerkt,[340] de naleving van technische vereisten en de keuringsprocedure,[341] logging en de beveiliging van gegevens en de manier waarop deze worden gebruikt, bewaard en vernietigd.[342] Het toezicht richt zich niet alleen op de fase nadat een opsporingsonderzoek heeft plaatsgevonden, maar de Inspectie kan ook steekproefsgewijs meekijken in de praktijk bij het daadwerkelijk binnendringen en onderzoek doen in een geautomatiseerd werk.[343] Haar bevindingen legt de Inspectie jaarlijks vast in een openbaar Verslag.[344] Indien structurele problemen worden geconstateerd, kan zij de politie vragen een 'verbeterplan' op te stellen. Ook kan besloten worden om het toezicht op sommige terreinen verder 'te intensiveren'.[345]

De taken van de Inspectie hebben betrekking op de uitvoering (vindt de inzet plaats volgens 'relevante wet- en regelgeving en binnen de kaders van het bevel van de officier van justitie en de machtiging van de rechter-commissaris'),[346] maar zij toetst niet de rechtmatigheid van de concrete inzet. Dat is aan de rechter ter terechtzitting.[347]

Procureur-generaal bij de Hoge Raad
De Inspectie houdt ook geen toezicht op het handelen van het Openbaar Ministerie. Dat gebeurt door de procureur-generaal bij de Hoge Raad (hierna PG-HR). De Inspectie kan wel de PG-HR op de hoogte stellen wanneer sprake is van 'schendingen van wettelijke voorschriften door of in opdracht van de officier van justitie'.[348] In september 2022 heeft de PG-HR een eerste toezichtsrapport uitgebracht waarin zij de toepassing van de hackbevoegdheid en het handelen van het Openbaar Ministerie heeft onderzocht (Aben & Luining 2022).

Notificatieplicht, processen-verbaal en dossier
In navolging op de regeling voor de notificatie van bijzondere opsporingsbevoegdheden[349] bestaat ten aanzien van de hackbevoegdheid de verplichting om betrokkenen op de hoogte te brengen dat de bevoegdheid is ingezet. Dit betekent dat degene wiens geautomatiseerd werk is binnengedrongen in kennis moet worden gesteld dat een inzet heeft plaatsgevonden.[350] Ook wanneer een geautomatiseerd werk in het buitenland wordt binnengedrongen is in principe notificatie vereist.[351] Notificatie is niet nodig als het proces-verbaal van de toepassing van de bevoegdheid is toegevoegd aan de processtukken.[352]
In het Besluit staat vastgelegd van welke activiteiten de officier van justitie een proces-verbaal dient op te maken: (1) onregelmatigheden die zich voordoen gedurende de gegevensverzameling;[353] (2) plaatsing van het technisch hulpmiddel, inclusief eventuele onregelmatigheden;[354] (3) verrichten van onderzoekshandelingen, inclusief eventuele onregelmatigheden;[355] (4) verwijdering van een technisch hulp-

340 *Kamerstukken II* 2017/18, 34 372, nr. 27.
341 Besluit onderzoek in een geautomatiseerd werk, 2018.
342 *Kamerstukken I* 2016/17, 34 372, D.
343 Besluit onderzoek in een geautomatiseerd werk, 2018, p. 24.
344 Inspectie JenV (2020); Inspectie JenV (2021); Inspectie JenV (2022).
345 *Kamerstukken I* 2017/18, 34 372, G.
346 *Kamerstukken I* 2017/18, 34 372, G.
347 *Kamerstukken II* 2016/17, 34 372, nr. 6.
348 *Kamerstukken II* 2016/17, 34 372, nr. 6.
349 Artikel 126bb Sv.
350 *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 40.
351 *Kamerstukken II* 2016/17, 34 372, nr. 6.
352 *Kamerstukken II* 2016/17, 34 372, nr. 6.
353 Artikel 6, lid 2 Bogw.
354 Artikel 23, lid 3 en 4 Bogw.
355 Artikel 24, lid 2 en 3 Bogw.

middel;[356] (5) niet volledige verwijdering van een technisch hulpmiddel;[357] en (6) selectie van gegevens indien bewerkingen hebben plaatsgevonden.[358] Het streven is om de handelingen die Digit verricht 'zo spoedig' mogelijk vast te leggen in een proces-verbaal.[359] In verband met de afscherming van onderzoeksmethoden kan gekozen worden voor een verantwoording die minder gedetailleerd is. Het is aan de officier van justitie om hier een oordeel over te vellen.[360]

De officier van justitie bepaalt welke stukken uit het politiedossier in het procesdossier terecht komen. Zodra een gerechtelijk vooronderzoek gesloten of geëindigd is, mag het kennisnemen van alle processtukken (oorspronkelijk of in afschrift) de verdachte niet worden onthouden. Dat geldt ook voor situaties waarin een gerechtelijk voor-onderzoek niet heeft plaatsgehad, zodra het kennisgeven van verdere vervolging of de dagvaarding ter terechtzitting in eerste aanleg aan de verdachte is betekend dan wel een strafbeschikking is uitgevaardigd.[361] Bij Algemene Maatregel van Bestuur wordt de wijze geregeld waarop de kennisneming van processtukken mag geschieden.[362] De verdachte kan bij de griffie een afschrift krijgen van stukken waarvan kennisneming hem of haar is toegestaan. Het onderzoek mag daardoor niet worden opgehouden.[363] Bij Algemene Maatregel van Bestuur worden regels gesteld met betrekking tot het verstrekken van afschriften en uittreksels.[364]

Jurisprudentie
In de periode maart 2019 t/m maart 2021 zijn in 26 opsporingsonderzoeken bevelen afgegeven voor de inzet van de hackbevoegdheid (Van Uden & Van de Eeden, 2022, p. 12). Voor zover bekend is de inzet van de hackbevoegdheid (tot nu toe) nog géén onderwerp van gesprek geweest tijdens de behandeling van een zaak in de rechtbank. Enkele zaken waarbij een poging is gedaan de hackbevoegdheid in te zetten of de hackbevoegdheid is ingezet zijn wel inmiddels inhoudelijk behandeld in de rechtszaal (zie bijvoorbeeld Berndsen (2022)).

Keuring in de praktijk
Een belangrijke aanleiding voor dit rechtsvergelijkend onderzoek was een eerste Verslag van de Inspectie op basis waarvan de Minister van Justitie en Veiligheid concludeerde dat de inzet van technische hulpmiddelen en de keuring ervan nog niet verliep zoals volgens het wettelijk kader was bedoeld. Inmiddels is op basis van een eerste evaluatie door het WODC meer duidelijk geworden over de vraag hoe de keuring in de praktijk verloopt en welke knelpunten de opsporingspraktijk ervaart met betrekking tot de inzet van technische hulpmiddelen en de keuring ervan. In deze paragraaf zetten we de belangrijkste bevindingen in dat kader op een rij. Een overzicht hiervan is van belang om op zinvolle wijze een vergelijking tussen Nederland en het buitenland te kunnen maken (zie hoofdstuk 8).
Op dit moment keurt de landelijke keuringsdienst (hierna Keuringsdienst) de tech-nische hulpmiddelen die de politie ontwikkelt. Deze dienst opereert onafhankelijk, maar maakt, net zoals Digit-politie, onderdeel uit van de Landelijke eenheid van de Nationale Politie. De Keuringsdienst keurt ook de meer traditionele technische hulpmiddelen (zoals bedoeld in het Besluit technische hulpmiddelen strafvordering).

[356] Artikel 25, lid 3 Bogw.
[357] Artikel 26, lid 3 Bogw.
[358] Artikel 29, lid 3 Bogw.
[359] *Kamerstukken II* 2016/17, 34 372, nr. 3, p. 78.
[360] Besluit onderzoek in een geautomatiseerd werk, p. 22.
[361] Artikel 33 Sv.
[362] Artikel 34 lid 1 Sv.
[363] Artikel 34 lid 2 Sv.
[364] Artikel 34 lid 1 Sv.

Denk daarbij aan bakens die onder een auto worden geplaatst, of camera's die worden gebruikt om verdachten te kunnen observeren. De Keuringdienst hanteert bij haar keuringen van technische hulpmiddelen die bedoeld zijn voor de hackbevoegdheid een keuringsprotocol gebaseerd op het Besluit. Dit protocol bestaat uit zeventien eisen en aan elke eis zijn meerdere normen verbonden. In het totaal kent het protocol 56 normen. Het volledige keuringsprotocol is niet openbaar, maar in het protocol wordt bijvoorbeeld aandacht besteed aan de wijze waarop de transportbeveiliging geregeld moet zijn.

Keuring van eigen technische hulpmiddelen
Digit heeft de afgelopen twee jaar enkele keren gebruikt gemaakt van een eigen (door de politie zelf) ontwikkeld technisch hulpmiddel. In het overgrote deel van de opsporingsonderzoeken werd gebruikt gemaakt van een commercieel product (hierover later meer). In de door ons onderzochte periode (maart 2019- april 2021) zijn drie technische hulpmiddelen ontwikkeld waarvan de Keuringsdienst er twee goedgekeurd heeft.[365] De ontwikkeling van een (goed-)gekeurd technisch hulpmiddel neemt veel tijd in beslag. Het ontwikkelen van een (eerste versie van een) technisch hulpmiddel duurt al gauw vier weken (indien sprake is van een eenvoudig technisch hulpmiddel). Nadat een hulpmiddel klaar is, moet het gekeurd worden. Dat traject duurt ook minimaal vier weken, maar vaker is meer tijd nodig, al gaan inmiddels de keuringen sneller dan vlak na de inwerkingtreding van de wet. Omdat het (nog) niet is voorgekomen dat een hulpmiddel in één keer goedgekeurd werd, worden daarna nog één of meerdere versies ontwikkeld, inclusief per versie een nieuw keuringstraject. Alles bij elkaar duurt het minstens vier maanden om goedkeuring te krijgen voor een middel, of er komt helemaal geen goedkeuring. In de praktijk blijkt het dus lastig om een vooraf goedgekeurd hulpmiddel in te zetten. Digit worstelt met het feit dat een aangepast middel volledig opnieuw moet worden gekeurd. De Keuringsdienst keurt een aangepast middel opnieuw, omdat alleen dan uitspraken kunnen worden gedaan over de werking van het middel en over de vraag of daarmee gegevens worden verzameld die betrouwbaar, herleidbaar en integer zijn.

Los van de keuringstermijn vormt de keuring in meer algemene zin een belangrijk knelpunt voor Digit. Dat heeft te maken met het feit dat de Keuringsdienst en Digit vanuit verschillende perspectieven naar het keuringsproces kijken. Vanuit het perspectief van de Keuringsdienst, staan vooral de regels centraal: een hulpmiddel kan, zoals volgt uit het wettelijk kader, alleen goedgekeurd worden als aan *alle* eisen uit het keuringsprotocol wordt voldaan (eventueel aangevuld met vervangende waarborgen). Voor de Keuringsdienst is dit belangrijk, omdat op die manier de betrouwbaarheid, integriteit en herleidbaarheid van gegevens gegarandeerd kunnen worden. De Keuringsdienst wil bij de rechter kunnen verklaren dat niks veranderd is aan de gegevens die bij een verdachte zijn opgehaald en dat kan alleen als aan alle eisen is voldaan.

Vanuit het perspectief van Digit wordt in de keuring vooral gekeken naar de uitvoerbaarheid en de noodzakelijkheid van de regels en de daarop gebaseerde eisen. Digit vindt de regels en eisen lastig uitvoerbaar, onder andere omdat ze niet goed zouden passen bij de hulpmiddelen die Digit ontwikkelt. De redenering is dat de regels in het Besluit (en het daarop gebaseerde keuringsprotocol) vooral gebaseerd zijn op het 'oude' Besluit dat gericht is op traditionele technische hulpmiddelen en deze

[365] De Inspectie JenV (2022, p. 7) schrijft in haar derde Verslag dat Digit in twee zaken een vooraf goedgekeurd technisch hulpmiddel heeft ingezet. Verder zijn in 2021 zeven technische hulpmiddelen ter keuring aangeboden en vijf technische hulpmiddelen goedgekeurd.

traditionele technische hulpmiddelen bestaan lang niet altijd uit software. Door vooral het 'oude' Besluit als uitgangspunt te nemen, zou er vanuit worden gegaan dat Digit de volledige controle kan hebben over de omgeving waarin een technisch hulpmiddel geplaatst wordt, vergelijkbaar met een baken waarvan de politie zelf de instellingen beheert. Controle van de omgeving en de handelingen die een verdachte daarbinnen verricht is voor de opsporingspraktijk echter lang niet altijd mogelijk. Digit kan bijvoorbeeld niet zelf de instellingen van het geautomatiseerd werk van de verdachte beheren[366] of bepalen over welke soort verbinding de verdachte gegevens binnenhaalt. Daarnaast heeft Digit géén invloed op wat een verdachte met zijn of haar geautomatiseerd werk doet. Als deze zijn geautomatiseerd werk uitzet, dan is dat problematisch voor de tijdsregistratie en de logging die eigenlijk continu zouden moeten plaatsvinden. Vervolgens is het lastig om aan te tonen dat de kwaliteit van de verzamelde gegevens op orde is.

Digit acht ook niet alle regels noodzakelijk, omdat te weinig rekening zou worden gehouden met risicoanalyses en bewijswaardes. Werken op basis van risicoanalyses betekent dat een inschatting wordt gemaakt wat de consequenties zijn als een technisch hulpmiddel niet volledig aan één of meerdere eisen voldoet. Dat zal niet altijd een probleem zijn, zo redeneert Digit, bijvoorbeeld wanneer de kans heel erg klein is dat het niet volledig voldoen aan een eis risico's oplevert voor de kwaliteit van het bewijs dat verzameld wordt. Digit is daarnaast van mening dat 100% betrouwbaarheid niet koste wat kost moet worden nagestreefd, omdat bewijs op verschillende manieren wordt gewogen. Niet alle gegevens die met behulp van een (bijzondere) opsporingsbevoegdheid worden verzameld, worden gebruikt als bewijs, bijvoorbeeld in het geval van sturingsinformatie. Mochten de gegevens wel worden gebruikt als bewijs, dan vindt de veroordeling van een verdachte doorgaans plaats op basis van verschillende stukjes bewijs, dikwijls verzameld met behulp van diverse (bijzondere) opsporingsbevoegdheden. Niet elk stukje van dit bewijs zal beschikken over dezelfde bewijswaarde.

Keuring van commerciële producten
In de meerderheid van de opsporingsonderzoeken waarin de bevoegdheid is ingezet is gebruikgemaakt van een commercieel product waarvan de landelijk Digit-officier van justitie besloten heeft dat de aard ervan zich tot nu toe verzet tegen een keuring. Aan die beslissing ligt een aantal argumenten ten grondslag. In de eerste plaats de updatesnelheid van het product. De gemiddelde updatesnelheid zou ongeveer zes tot acht dagen zijn. De vraag is welke versie(s) de Keuringsdienst moet keuren. En mochten alle versies worden gekeurd, dan past dat niet bij de doorlooptijd die een keuring doorgaans in beslag neemt. Ten tweede het bedrijfsgeheim van de leverancier. De werking van een commercieel product is voor de opsporingspraktijk een 'zwarte doos'. Dat betekent dat ook de Keuringsdienst geen exacte inzage kan krijgen in de wijze waarop het product werkt. Het derde argument heeft te maken met het feit dat de leverancier te allen tijde toegang wil hebben tot zijn product, bijvoorbeeld voor het plegen van onderhoud. Daardoor krijgt de Keuringsdienst geen exclusieve toegang tot het middel, hetgeen voor haar een vereiste is om de keuring te kunnen doen.

[366] Denk daarbij aan de tijdsinstelling van het geautomatiseerd werk.

Bijlage 5 Samenstelling begeleidingscommissie

Voorzitter

Prof. mr. dr. M.F.H. (Marianne) Hirsch Ballin	Hoogleraar Straf- en Strafprocesrecht, Vrije Universiteit Amsterdam

Leden

Mr. K. (Koen) Hermans	Landelijk officier cybercrime, Openbaar Ministerie
Lec. dr. J. (Jurjen) Jansen	Lector Digitale Weerbaarheid, NHL Stenden
Dr. mr. D.A.G. (Dave) van Toor	Universitair docent straf(proces)recht, Universiteit Utrecht
Mr. M. (Madiha) Malik	Beleidsadviseur DGPenV, Ministerie van Justitie en Veiligheid

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is het kennisinstituut voor het ministerie van Justitie en Veiligheid. Het WODC doet zelf onafhankelijk wetenschappelijk onderzoek of laat dit doen door erkende instituten en universiteiten, ter ondersteuning van beleid en uitvoering.

Meer informatie:

www.wodc.nl