# Toezicht op buitenlandse inlichtingen- en veiligheidsdiensten: rapport 2025

Oerlemans, J.J.

# TOEZICHT OP BUITENLANDSE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

RAPPORT

# 2025

mr. dr. Jan-Jaap Oerlemans

Universiteit Leiden
Instituut voor Strafrecht en Criminologie

COLOFON


| | |
|---|---|
| Titel: | *Toezicht op buitenlandse inlichtingen- en veiligheidsdiensten* |
| Uitgevoerd door: | De afdeling Strafrecht van het Instituut Strafrecht & Criminologie van de Universiteit Leiden |
| Auteur: | mr. dr. Jan-Jaap Oerlemans<br>Met medewerking van mr. Naomi Stal |
| Opdrachtgever: | Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Defensie |
| Publicatiegegevens: | Juli 2025, Leiden: Universiteit Leiden |

Citatiewijze:
J.J. Oerlemans, 'Toezicht op buitenlandse inlichtingen- en veiligheidsdiensten', Universiteit Leiden, juli 2025

# Inhoudsopgave

Samenvatting ..... 4
Lijst met afkortingen ..... 6
Hoofdstuk 1: Inleiding ..... 7
1.1 Onderzoeksvragen ..... 7
1.2 Methodologie ..... 8
1.3 Leeswijzer ..... 9
Hoofdstuk 2: Normatief kader voor toezicht op bulkinterceptie ..... 10
2.1 Vereisten van toezicht op bulkinterceptie ..... 10
2.1.1 Big Brother Watch ..... 11
2.1.2 Centrum för Rättvisa ..... 14
2.1.3 Association Contrafraternelle de la Presse Judiciaire e.a. ..... 17
2.2 Vereisten voor toezicht op gegevensverwerking ..... 20
2.2.1 Inleiding Conventie 108+ ..... 20
2.2.2 Betekenis van Conventie 108+ in het nationale veiligheidsdomein ..... 21
2.2.3 Uitzonderingen op de verdragsbepalingen ..... 22
2.3 Integratie van de vereisten voor toezicht ..... 22
2.3.1 Onafhankelijkheid en effectiviteit ..... 22
2.3.2 Formele toezichthouders en overige toezichthouders ..... 23
2.3.3 Fasen van toezicht ..... 24
2.4 Conclusie ..... 26
Hoofdstuk 3: Het toezichtstelsel in Denemarken ..... 28
3.1 De inlichtingen- en veiligheidsdiensten van Denemarken ..... 28
3.1.1 PET ..... 28
3.1.2 FE ..... 28
3.1.3 CFCS ..... 29
3.2 De uitoefening van bulkinterceptie in Denemarken ..... 30
3.2.1 Bulkinterceptie en toezicht van 2013-2025 ..... 30
3.2.2 Wetsvoorstel ‘Versterking van het toezicht op de Deense inlichtingendiensten’ 31
3.3 Het stelsel van toezicht ..... 33
3.3.1 De Inlichtingenraad ..... 34
3.3.2 TET ..... 34
3.3.3 Het College van toezicht op de inzagerechten ..... 37

3.3.4 Overige toezichthouders ..... 38
3.4 Conclusie ..... 39
Hoofdstuk 4: Het toezichtstelsel in Zweden ..... 41
4.1 De inlichtingen- en veiligheidsdiensten van Zweden ..... 41
4.1.1 SÄPO ..... 41
4.1.2 MUST ..... 42
4.1.3 FRA ..... 42
4.1.4 Nationaal cybersecuritycentrum ..... 43
4.2 De uitoefening van bulkinterceptie in Zweden ..... 43
4.2.1 Ontwikkeling juridisch kader voor bulkinterceptie ..... 43
4.2.2 Ex ante autorisatie ..... 44
4.2.3 Ex post toezicht ..... 44
4.3 Het stelsel van toezicht ..... 46
4.3.1 Het Defensie Inlichtingenhof ..... 46
4.3.2 Siun ..... 47
4.3.4 IMY ..... 48
4.3.3 Sin ..... 49
4.3.5 Overige toezichthouders ..... 49
4.4 Conclusie ..... 50
Hoofdstuk 5: Het toezichtstelsel in Frankrijk ..... 52
5.1 De inlichtingen- en veiligheidsdiensten van Frankrijk ..... 52
5.1.1 DGSE ..... 52
5.1.2 DGSI ..... 53
5.1.3 DNRED ..... 53
5.1.4 DRM ..... 53
5.1.5 DRSD ..... 53
5.1.6 Tracfin ..... 54
5.1.7 ANSSI ..... 54
5.2 De uitoefening van bulkinterceptie in Frankrijk ..... 54
5.2.1 Ontwikkeling juridisch kader voor bulkinterceptie ..... 55
5.2.2 Ex ante toestemming ..... 56
5.2.3 Beroepsprocedure ..... 57
5.2.4 Ex post toezicht ..... 57
5.3 Het stelsel van toezicht ..... 58

5.3.1 CNCTR ..... 58
5.3.2 Conseil D'État ..... 59
5.3.3 Overige toezichthouders ..... 60
5.4 Conclusie ..... 61
Hoofdstuk 6: Het toezichtstelsel in het Verenigd Koninkrijk ..... 62
6.1 De inlichtingen- en veiligheidsdiensten van het Verenigd Koninkrijk ..... 62
6.1.1 MI5 ..... 62
6.1.2 SIS (MI6) ..... 63
6.1.3 GHCQ ..... 63
6.1.4 National Cyber Security Centre (NCSC) ..... 64
6.2 De uitoefening van bulkinterceptie in het Verenigd Koninkrijk ..... 64
6.2.1 De ontwikkelingen n.a.v. *Big Brother Watch* ..... 65
6.2.2 Ex ante toestemming ..... 66
6.2.3 Ex durante toezicht ..... 67
6.2.4 Ex post toezicht ..... 67
6.2.5 Effectief rechtsmiddel ..... 68
6.3 Het stelsel van toezicht ..... 68
6.3.1 IPCO ..... 68
6.3.2 IPT ..... 70
6.3.3 De verhouding tussen IPCO en IPT ..... 71
6.3.4 Overige toezichthouders ..... 71
6.4 Conclusie ..... 72
Hoofdstuk 7: Conclusie ..... 74
Geraadpleegde literatuur ..... 79
Jurisprudentie ..... 86

# Samenvatting

Dit rapport beantwoordt de vraag hoe de toetsings- en toezichtsystemen op inlichtingen- en veiligheidsdiensten zijn ingericht in Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk. Hiervoor is een normatief kader opgesteld op basis van jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en de vereisten uit het gemoderniseerde gegevensbeschermingsverdrag 'Conventie 108+'.

De uitspraken van de Grote Kamer van het EHRM in de zaken *Big Brother Watch e.a.* en *Centrum för Rättvisa e.a.* uit 2021 hebben aanzienlijke gevolgen gehad voor de onderzochte landen. In 2025 hebben de Zweedse en Deense regeringen wetsvoorstellen ingediend om het toezicht te versterken en tegelijkertijd de bevoegdheden voor het verzamelen en verwerken van bulkdatasets wettelijk vast te leggen.

Uit deze jurisprudentie en verdragen blijkt dat onafhankelijk en effectief toezicht noodzakelijk is in alle fasen van de inzet van bulkinterceptie als inlichtingenmiddel. Dat wil zeggen: (1) vooraf (*ex ante*) door middel van een rechtmatigheidstoets op de inzet door een onafhankelijke instantie of rechter; (2) tijdens (*ex durante*) door middel van doorlopend toezicht met geautomatiseerde controlesystemen; (3) en achteraf (*ex post*) via inspecties of steekproeven door een gespecialiseerde toezichthouder of rechter. Het EHRM benadrukt in de beslissing *Contrafraternelle de la Presse Judiciaire* uit 2024 ook het belang van een effectief rechtsmiddel (de 'remedy') in het stelsel van toezicht op inlichtingen- en veiligheidsdiensten. Het EHRM vereist dat de beslissingen van de onafhankelijke instantie of rechter met redenen omkleed en juridisch bindend zijn, bijvoorbeeld door de mogelijkheid tot het bevelen van de vernietiging van onrechtmatig verwerkte gegevens.

Het EHRM hanteert bij de beoordeling van nationale toezichtstelsels een zogenoemde 'holistische benadering'. Daarbij wordt niet alleen gekeken aan afzonderlijke vereisten bij de inzet van vergaande bevoegdheden zoals bulkinterceptie als inlichtingenmiddel, maar vooral naar de effectiviteit van het stelsel als geheel. Het toezicht op de inzet van vergaande bevoegdheden zoals bulkinterceptie door inlichtingen- en veiligheidsdiensten kan daardoor per land sterk verschillen. Dat blijkt ook uit dit rapport en eerdere onderzoeken die in Europees verband naar dit onderwerp zijn uitgevoerd.

Hoewel alle onderzochte landen bulkinterceptie inzetten ter bescherming van de nationale veiligheid, verschillen hun toezichtstelsels aanzienlijk. Frankrijk en het Verenigd Koninkrijk beschikken over één gespecialiseerde toezichthouder die toezicht houdt op alle fasen van het proces bij een groot aantal diensten (circa 20 in Frankrijk en meer dan 600 in het Verenigd Koninkrijk). Verder is het kenmerkend voor Frankrijk en het Verenigd Koninkrijk dat gespecialiseerde rechtsinstanties klachten behandelen over vermeend onrechtmatig handelen door de inlichtingen- en veiligheidsdiensten. De wetgeving in deze landen bevat gedetailleerde bepalingen over de procedure bij hoorzittingen, de toegang tot staatsgeheimen en de bevoegdheden om bindende beslissingen te nemen. Het EHRM oordeelt dat deze landen voorzien in een 'robuust' en effectief rechtsmiddel.

In Zweden houden verschillende gespecialiseerde toezichthouders tegelijk toezicht op de Zweedse inlichtingen- en veiligheidsdiensten. Een onafhankelijke rechtsinstantie voert vooraf een rechtmatigheidstoets uit voordat bulkinterceptie mag plaatsvinden. In Denemarken ontbreekt vooralsnog een dergelijke ex ante-toets. Ook ontbreekt daar gedetailleerde

regelgeving over de inzet van bulkinterceptie, en richt het toezicht zich vooral op gegevensverwerking. Bovendien is het toezicht vaak beperkt tot personen en rechtspersonen die in Denemarken verblijven. Een wetsvoorstel uit 2025 beoogt hierin verandering te brengen. De toezichthouder TET zou een breder mandaat krijgen door het toezicht uit te breiden naar operationele activiteiten. Daarnaast worden de (bulk)bevoegdheden in het wetsvoorstel voor inlichtingen- en veiligheidsdiensten vergroot, en krijgt TET een 'College van toezicht op de inzagerechten' met bindende bevoegdheden, waartegen geen beroep mogelijk is.

In Zweden en Denemarken is ervoor gekozen een afdeling voor klachtbehandeling toe te voegen binnen de bestaande toezichthouder. Deze keuze is ingegeven door veiligheidsredenen (de omgang met staatsgeheime informatie), de specialistische kennis van de medewerkers en commissieleden van deze toezichthouders, en efficiëntie (zoals het delen van een secretariaat en infrastructuur). In Frankrijk worden klachten eveneens door de toezichthouder behandeld, met een beroepsmogelijkheid bij de hoogste bestuursrechter. Frankrijk is het enige land waar de toets vooraf op de inzet van vergaande bevoegdheden, het toezicht tijdens en achteraf, én de behandeling van klachten zijn ondergebracht bij één en dezelfde specialistische toezichthouder op de inlichtingen- en veiligheidsdiensten.

Tijdens het onderzoek viel op dat elk van de onderzochte landen beschikt over een nationaal cybersecuritycentrum, waarvan de meeste een sterke relatie hebben met de nationale SIGINT-organisatie (bijvoorbeeld door inbedding van het centrum binnen deze organisatie). Niet alle cybersecuritycentrums vallen echter onder specialistisch toezicht, ondanks hun bevoegdheid in meer of mindere mate internetverkeer te monitoren. Daarbij is sprake van een inmenging met fundamentele rechten, zoals het recht op privacy en het recht op gegevensbescherming, veelal zonder een gedetailleerde wettelijke regeling en toezicht op deze activiteiten. Denemarken is het enige land waar de toezichthouder expliciet toezicht houdt op het cybersecuritycentrum en daarover jaarlijks rapporteert. In het Verenigd Koninkrijk valt het nationale cybersecurity centrum (NCSC) onder de communicatie-inlichtingendienst, die op haar beurt onder toezicht staat van een gespecialiseerde toezichthouder.

Vervolgonderzoek zou zich kunnen richten op het toezichtstelsel in andere landen of op andere overheidsinstanties die zich bezighouden met opsporing of het verzamelen van inlichtingen in andere domeinen, zoals het opsporings- of het fiscale inlichtingendomein. Dit rapport richt zich op de nationale dimensie van het toezicht op inlichtingen- en veiligheidsdiensten, terwijl deze diensten ook intensief kunnen samenwerken, bijvoorbeeld via gezamenlijke operaties, gegevensuitwisseling of gezamenlijke gegevensverwerkingen. Dit alles vindt plaats terwijl het toezicht nationaal is geregeld. Nader onderzoek zou zich daarom kunnen richten op de noodzaak van toezicht op gezamenlijke inlichtingenoperaties.

# Lijst met afkortingen

AIVD: Algemene Inlichtingen- en Veiligheidsdienst
ANSSI: *Agence nationale de la sécurité des systèmes d'information*
ARCEP: *Autorité de régulation des communications électroniques et des postes*
CERT: *Computer Emergency Response Team*
CFCS: *Center for Cybersikkerhed*
CNCTR: *Commission nationale de contrôle des techniques de renseignement*
CNE: *Computer Network exploitation*
DCAF: *Centre for Security Sector Governance*
DGSE: *Direction générale de la sécurité extérieure*
DGSI: *Direction générale de la sécurité intérieure*
DNRED: *Direction nationale du renseignement et des enquêtes douanières*
DRM: *Direction du renseignement militaire*
DRSD: *Direction du renseignement et de la sécurité de la défense*
EHRM: Europees Hof voor de Rechten van de Mens
EVRM: Europees Verdrag voor de Rechten van de Mens
FE: *Forsvarets Efterretningstjeneste*
FRA: *Försvarets radioanstalt*
GCHQ: *Government Communications Headquarters*
GEOINT: *Geospatial Intelligence*
GIC: *Groupement Interministériel de Controle*
HUMINT: *Human Intelligence*
IMINT: *Imagery Intelligence*
IMY: *Integritetsskyddsmyndigheten*
IPA: *Investigatory Powers Act 2024*
IPCO: *Investigatory Powers Commissioner's Office*
ISC: *Intelligence and Security Committee*
MI5: *Security Service*
MIVD: Militaire Inlichtingen- en Veiligheidsdienst
MSB: *Myndigheten för samhällsskydd och beredskap*
NAO: *National Audit Office*
NCSC: *National Cyber Security Centre*
NGO: non-gouvernementele organisatie
OSINT: *Open Source Intelligence*
PET: *Politiets Efterretningstjeneste*
PNR: *Passenger Name Records*
RIPA: *Regulation of Investigatory Powers Act*
SGDSN: *Secrétariat général de la défense et de la sécurité nationale*
SIGINT: S*ignals Intelligence*
SIS (ook: MI6): *Secret Intelligence Service*
Sin: *Säkerhets- och integritetsskyddsnämnden*
Siun: *Statens inspektion för försvarsunderrättelseverksamheten*
SÄPO: *Säkerhetspolisen*
TAP: *Technology Advisory Panel*
TECHINT: *Technical Intelligence*
TET: *Tilsynet med Efterretningstjenesterne*
Tracfin: *Traitement du renseignement et action contre les circuits financiers clandestins*
Wiv 2017: Wet op de inlichtingen- en veiligheidsdiensten

# Hoofdstuk 1: Inleiding

Op 5 maart 2021 reageerden de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie op het evaluatierapport van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017.[1] Het toenmalige kabinet heeft destijds besloten tot dat er aanleiding was tot een herziening van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017).[2] De herziening heeft mede tot doel te komen tot een beter functionerend stelsel van toetsing en toezicht op de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

Het onderhavige rapport betreft een onderzoek naar de toezichtstelsels van Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Defensie. Deze landen zijn door de opdrachtgevers geselecteerd, omdat ze regelmatig als voorbeeld worden aangehaald in het parlementair debat over toezicht op de diensten en binnen een vergelijkbaar juridisch kader opereren.

Dit rapport verschaft een overzicht van de wet- en regelgeving, de organisatorische structuren en de uitvoeringspraktijken van de toetsingsinstanties en toezichthouders in Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk. De uitkomsten van dit onderzoek kunnen worden gebruikt in de voorbereiding van het wetstraject voor de herziening van de Wiv 2017.

## 1.1 Onderzoeksvragen

De centrale onderzoeksvraag luidt als volgt:

*Hoe zijn de toezichtstelsels op inlichtingen- en veiligheidsdiensten ingericht in Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk?*

Daarop zijn de volgende deelvragen geformuleerd:

- *Wat zijn de wettelijke kaders voor het werk van de diensten en hun toezichthouders?*
- *Welke toetsing- en toezichthoudende instanties zijn betrokken en welke vormen van toezicht (parlementair, rechterlijk, specialistisch) oefenen zij uit?*
- *Wat is de rol van de rechter, en bestaat er een beroepsmogelijkheid binnen het stelsel?*
- *Hoe typeert de toetsing en het toezicht zich (ex ante, ex durante, ex post) en hoe verhouden de instanties zich tot elkaar?*
- *Over welke onderdelen van de taakuitvoering – en de bevoegdheden in het bijzonder - van de diensten zijn deze instanties bevoegd te oordelen?*
- *Welke bevoegdheden en middelen hebben toezichthouders voor hun taken?*
- *Welke maatregelen kunnen toezichthouders nemen, en zijn deze bindend?*

[1] Brief van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie van 5 maart 2021, *Kamerstukken II* 34 588, nr. 89.

[2] Brief van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie van 17 juni 2025 over de stand van zaken Herziening Wet op de inlichtingen- en veiligheidsdienst (*Kamerstukken II* 34 588, nr. 94). In deze Kamerbrief is te lezen dat ‘in de context van de internationale dreiging en in het belang van de nationale veiligheid het demissionaire kabinet ernaar blijft streven het wetsvoorstel begin 2026 voor consultatie aan te bieden gevolgd door de adviesaanvraag bij de Afdeling advisering van de Raad van State’.

## 1.2 Methodologie

De onderzoeksvraag is beantwoord door middel van klassiek juridisch onderzoek. Dat wil zeggen dat een literatuurstudie is uitgevoerd met betrekking tot het toezicht op de inlichtingen- en veiligheidsdiensten van de genoemde landen, jurisprudentie over toezicht op inlichtingen- en veiligheidsdiensten is bestudeerd, en de wet- en regelgeving uit deze landen is onderzocht. Daarbij is gebruik gemaakt van wetenschappelijke literatuur en 'grijze literatuur', zoals rapporten van de toezichthouders en evaluatiecommissies.

*Achtergrondgesprekken*

Na afronding van het literatuuronderzoek zijn achtergrondgesprekken gevoerd met vertegenwoordigers van toezichthoudende instanties uit de betrokken landen. Deze gesprekken dienden met name voor het identificeren van relevante bronnen en de status van recente of aankomende wetgeving te verifiëren. Deze gesprekken leverden waardevolle inzichten op, vooral over recent gepubliceerde wetsvoorstellen. In enkele voetnoten wordt verwezen naar deze achtergrondgesprekken. De betreffende passages zijn ter akkoord voorgelegd aan de betrokken personen.

Onderstaande lijst geeft een overzicht van de gesprekspartners en hun organisaties. In enkele gevallen worden namen om veiligheidsredenen niet vermeld:

- Emil Bock Greve, directeur, *Tilsynet med Efterretningstjenesterne* (TET)
- Twee adviseurs, *Säkerhets- och integritetsskyddsnämnden* (SIN)
- Twee adviseurs, *Statens inspektion för försvarsunderrättelseverksamheten* (Siun)
- Adviseur van de voorzitter, *Commission nationale de contrôle des techniques de renseignement* (CNCTR)
- Richard Thompson, Chief Executive Officer, en twee adviseurs, *Investigatory Powers Commissioner's Office* (IPCO)

De auteur spreekt zijn dank uit aan de betrokken toezichthouders voor hun bereidheid om aan deze gesprekken deel te nemen en hun inzichten te delen. Hun openheid en medewerking hebben bijgedragen aan de kwaliteit en actualiteit van dit onderzoek.

*Normatief kader*

Voordat het toezichtstelsel en de toetsingsmechanismen met betrekking tot de inlichtingen- en veiligheidsdiensten beschreven kunnen worden, is het noodzakelijk uit te leggen aan welk juridisch kader wordt getoetst. Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk zijn allen verdragsstaat bij het Europees Verdrag voor de Rechten van de Mens (EVRM) en daarmee gebonden aan de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM). Nederland, Zweden, Frankrijk en het Verenigd Koninkrijk hebben bovendien het Protocol bij Conventie 108 (hierna: Conventie 108+) ondertekend.[3] Kenmerkend is ook dat elk van deze landen bulkinterceptie als inlichtingenmiddel inzet.

In hoofdstuk 2 wordt het normatief kader met betrekking tot het toezicht op bulkinterceptie uitgewerkt op basis van jurisprudentie van het EHRM en de vereisten die voortvloeien uit

[3] Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, *Trb.* 2018, 201.

Conventie 108+. Dit leidt tot een model voor toezicht, dat wordt vergeleken met het toezichtstelsel van elk van de onderzochte landen. Voor zover deze informatie (publiekelijk) beschikbaar is, worden ook de bevoegdheden, beroepsmogelijkheden, en de middelen van de toezichthouders beschreven.

De belangrijkste beperking van dit onderzoek betreft de gekozen focus op het toezicht op inlichtingen- en veiligheidsdiensten die gebruikmaken van bulkinterceptie. Dit betekent onder meer dat het stelsel van toezicht op politiediensten en bijzondere opsporingsdiensten – die doorgaans gericht zijn op strafrechtelijke handhaving – buiten de reikwijdte van dit onderzoek valt. De nadruk ligt bovendien op het in kaart brengen van de instanties en bevoegdheden van de in dit onderzoek zogenoemde 'formele toezichthouders'. Hieronder worden gespecialiseerde toezichthouders en rechterlijke instanties verstaan. Nationale rekenkamers, parlementaire commissies en ombudsmaninstanties worden in dit rapport minder uitvoerig behandeld en aangemerkt als 'overige instanties'.

*Gebruik digitale hulpmiddelen*

Bij het opstellen van dit rapport is gebruikgemaakt van diverse digitale hulpmiddelen ter ondersteuning van vertaling, het opzoeken van informatie, het analyseren van informatie en tekstverbetering. Voor de vertaling van teksten zijn DeepL Pro en Microsoft Copilot ingezet. Voor het verbeteren van zinsstructuur, spelling en grammatica is gebruikgemaakt van het Gemma 3 12B-model via LM Studio en CoPilot. Daarnaast is NotebookLM van Google benut voor analyseren van rapporten en jurisprudentie. De auteur blijft verantwoordelijk voor eventuele onjuistheden of onvolkomenheden die onverhoopt in de tekst zijn achtergebleven.

## 1.3 Leeswijzer

Dit rapport is als volgt opgebouwd. Hoofdstuk 2 zet het normatief kader uiteen voor toezicht op bulkinterceptie. Vervolgens worden de deelvragen per land beantwoord, achtereenvolgens voor Denemarken (Hoofdstuk 3), Zweden (Hoofdstuk 4), Frankrijk (Hoofdstuk 5) en het Verenigd Koninkrijk (Hoofdstuk 6). In elk hoofdstuk worden de deelvragen beantwoord aan de hand van een beschrijving van de betrokken inlichtingen- en veiligheidsdiensten, het toezichtstelsel op bulkinterceptie, en de relevante toezichthouders.

Hoofdstuk 7 beantwoordt de centrale onderzoeksvraag en bespreekt opvallende verschillen in de toezichtsystemen van de onderzochte landen. Ook worden suggesties gedaan voor vervolgonderzoek.

# Hoofdstuk 2: Normatief kader voor toezicht op bulkinterceptie

Dit hoofdstuk beschrijft het normatief kader voor toezicht bij de inzet van bulkinterceptie door inlichtingen- en veiligheidsdiensten. De vereisten voor het toezicht worden afgeleid uit jurisprudentie van het EHRM ten aanzien van bulkinterceptie en de vereisten voor toezicht die voortvloeien uit Conventie 108+.

Paragraaf 2.1 beschrijft de vereisten voor het toezicht op bulkinterceptie, afgeleid uit jurisprudentie van het EHRM. De vereisten die volgen uit Conventie 108+ worden uiteengezet in paragraaf 2.2. In paragraaf 2.3 worden deze vereisten samengevoegd en uiteengezet ten aanzien van de verschillende fasen van toezicht: voorafgaand aan de inzet (*ex ante)*, tijdens de inzet (*ex durante*) en achteraf (*ex post*). De conclusie vervat deze vereisten in een toezichtsmodel ten aanzien van bulkinterceptie.

## 2.1 Vereisten van toezicht op bulkinterceptie

Inlichtingenmiddelen zoals bulkinterceptie maken een ernstige inbreuk op fundamentele rechten, met name op het recht op privacy in artikel 8 EVRM. Al in 1978 waarschuwde het EHRM in de zaak *Klass t. Duitsland* dat verdragsstaten geen onbeperkte discretionaire bevoegdheid hebben om het telecommunicatie- en postverkeer van personen binnen hun rechtsgebied in de gaten te houden. Het Hof wijst op het gevaar dat een dergelijke wet de democratie ondermijnt of zelfs vernietigt onder het mom van de verdediging ervan, en bevestigt dat de verdragsluitende staten niet in naam van de strijd tegen spionage en terrorisme alle maatregelen mogen nemen die zij passend achten.[4]

In daaropvolgende jurisprudentie oordeelde het EHRM ook over bulkinterceptie in de context van het onderscheppen van (mobiele) telefonie en ontwikkelde het vereisten voor wetgeving waar verdragstaten aan moeten voldoen om (met name) het recht op privacy in artikel 8 EVRM te respecteren.[5] Telkens voert het EHRM daarbij een driestaptoets uit: een inmenging op het recht op privacy kan gerechtvaardigd zijn, als die (1) een grondslag heeft in de wet, (2) een van de in artikel 8 lid 2 EVRM genoemde doeleinden nastreeft, en (3) in een democratische samenleving noodzakelijk is. Deze paragraaf richt zich op de vereisten van toezicht bij de inzet van bulkinterceptie door de inlichtingen- en veiligheidsdiensten van verdragsstaten ter bescherming van de nationale veiligheid.

Voor de bespreking van deze kwalitatieve vereisten ten aanzien van toezicht op bulkinterceptie ter bescherming van de nationale veiligheid worden achtereenvolgens de uitspraken geanalyseerd: *Big Brother Watch e.a.* tegen *het Verenigd Koninkrijk*, *Centrum för Rättvisa e.a.* tegen *Zweden*, en *Association Contrafraternelle de la Presse Judiciaire e.a.* tegen *Frankrijk*.[6]

---

[4] EHRM 6 september 1978, nr. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass t. Duitsland*).
[5] Zie, onder andere, EHRM 29 juni 2006, nr. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400 (*Weber en Saravia t. Duitsland*), *EHRC* 2007/13, m.nt. Loof; EHRM 1 juli 2008, nr. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300 (*Liberty e.a. t. het Verenigd Koninkrijk*), *EHRC* 2008/100, m.nt. Van der Velde; EHRM 18 mei 2010, nr. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905 (*Kennedy t. Verenigd Koninkrijk*), *EHRC* 2010/86; *NJ* 2011/333; EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), *NJ* 2017/185, m.nt. Dommering, *EHRC* 2016/87, m.nt. Hagens.
[6] EHRM (GK) 25 mei 2021, nr. 58170/13, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*) en EHRM (GK) 25 mei 2021, nr. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa t. Zweden*), *EHRC Updates* 2021, m.nt. M. Hagens & J.J. Oerlemans; *JBP* 2021/62, m.nt. E. Moyakine; *NJ* 2021/361, m.nt. E.J. Dommering, *NJB*

Deze uitspraken hebben een bepalende invloed gehad voor de vorming en wijzigingen van het toezicht in de betrokken landen in dit rapport.

### 2.1.1 Big Brother Watch

Op 25 mei 2021 deed de Grote Kamer van het EHRM uitspraak in de zaak *Big Brother Watch e.a.* tegen *het Verenigd Koninkrijk.*[7] Deze zaak ging over het in bulk verwerven van communicatie en de internationale uitwisseling van dergelijke gegevens door inlichtingen- en veiligheidsdiensten.[8] Specifiek ging het over de verzameling en verwerking van gegevens voor de *Government Communications Headquarters* (GHCQ). De GHCQ is de Britse communicatie-inlichtingendienst die verantwoordelijk is voor het leveren van signaalinlichtingen (*signals intelligence* (hierna: SIGINT)) en de informatiebeveiliging aan de regering en de strijdkrachten van het Verenigd Koninkrijk.

*Aanleiding*

Na de onthullingen van Edward Snowden in 2013 over het bestaan van grootschalige 'surveillance programs' van de inlichtingendiensten van de Verenigde Staten en het Verenigd Koninkrijk, zijn meerdere rechtszaken tegen het Verenigd Koninkrijk gevoerd. De zaak *Big Brother Watch e.a.* betreft drie gevoegde zaken naar aanleiding van klachten van journalisten en non-gouvernementele organisaties (ngo) die opkomen voor de fundamentele rechten van burgers, waaronder de ngo *Big Brother Watch*. De klagers meenden dat de aard van hun activiteiten met zich meebracht dat hun elektronische communicatie en gerelateerde communicatiegegevens (metadata) werden onderschept of waren verkregen door de inlichtingendiensten van het Verenigd Koninkrijk.

Het EHRM behandelde de klachten met als uitgangspunt de wetgeving die destijds in het Verenigd Koninkrijk gold. Deze 'Regulation of Investigatory Powers Act' (hierna: RIPA) is in de tussentijd aangepast (zie verder hoofdstuk 6). In *Big Brother Watch e.a.* gaat het onder andere over de verenigbaarheid van bulkinterceptie van 'buitenlandse communicatie' met artikel 8 van het EVRM.[9]

Het is van belang allereerst te benoemen dat het EHRM erkent dat de inzet van bulkinterceptie een legitiem doel kan hebben, omdat het van 'vitaal belang' voor verdragsstaten kan zijn om gekende en ongekende bedreigingen voor hun nationale veiligheid te identificeren.[10] Het Hof benadrukt dat de bedreigingen voor staten zijn versterkt door toegenomen digitalisering en technologische ontwikkelingen. Het Hof noemt ook expliciet het gevaar van bedreigingen op

---

2021/1804, m.nt. M.M. Groothuis; en EHRM 10 december 2024, nrs. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15, 59621/15, 30635/17, 30636/17, ECLI:CE:ECHR:2024:1210DEC004952615 (*Association Confraternelle de la Presse Judiciare et Autres t. Frankrijk*). Zie ook Oerlemans & Hagens 2019 en Jansen 2022.

[7] EHRM (GK) 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*). Daarvoor: EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), *Computerrecht* 2018/252, m.nt. J.J. Oerlemans; *EHRC* 2018/208, m.nt. M. Hagens.

[8] Deze beschrijving is deels afkomstig van de annotatie 'Legitimering bulkinterceptie' van M. Hagens en J.J. Oerlemans in *EHRC Updates* (laatst geraadpleegd op 15 juli 2025).

[9] De andere overwegingen van het EHRM over de verenigbaarheid met artikel 8 EVRM met betrekking tot de samenwerking tussen buitenlandse inlichtingen- en veiligheidsdiensten, de toegang van de Britse diensten tot opgeslagen communicatiegegevens (metadata) bij private communicatiediensten, en over de schending van artikel 10 EVRM (vrijheid van meningsuiting) komen hier verder niet aan bod.

[10] *Big Brother Watch e.a.,* par. 424.

cybersecuritygebied en noemt bulkinterceptie een "*valuable technological capacity to identify new threats in the digital domain*".[11]

Tegelijkertijd brengt bulkinterceptie een ernstige inbreuk op fundamentele rechten van betrokkenen met zich mee, en kan de onderschepte communicatie betrekking hebben op een groot aantal personen die geen onderwerp van onderzoek zullen zijn voor de inlichtingendiensten.[12] Kortgezegd moeten staten in voldoende waarborgen voorzien en zorg dragen voor toegankelijke en kenbare wettelijke normen. Bulkinterceptie mag slechts worden toegepast wanneer dit noodzakelijk is voor de bescherming van de democratische rechtsorde.

Het Hof herhaalt zijn overweging uit eerdere jurisprudentie dat een dergelijk surveillance-systeem, dat bedoeld is om de nationale veiligheid te beschermen, ook de democratie kan ondermijnen of zelfs vernietigen. Daarom moeten er voldoende waarborgen zijn om misbruik van een dergelijk verstrekkende bevoegdheid tegen te gaan. Het antwoord op de vraag of er voldoende waarborgen zijn hangt af van: de omstandigheden van het geval, de aard, de reikwijdte en de duur van de mogelijke maatregelen, de gronden die vereist zijn om ze te gelasten, de autoriteiten die bevoegd zijn om ze toe te staan, uit te voeren en te controleren, en het soort rechtsmiddel waarin de nationale wetgeving voorziet.[13] Nieuw is daarbij de overweging van het EHRM dat een systeem van bulkinterceptie moet voorzien in '*end-to-end safeguards*'. Deze waarborgen zijn een samenspel van de waarborgen van autorisatie, toezicht, en rechtsmiddelen.

*Autorisatie en toezicht als de hoeksteen van een bulkinterceptieregime*

Het EHRM benadrukt dat onafhankelijke autorisatie, toezicht op de uitvoering, en onafhankelijke *ex post facto*-toetsing fundamentele waarborgen zijn die de hoeksteen vormen van een bulkinterceptieregime dat verenigbaar is met artikel 8 EVRM.[14]

In de uitspraak *Big Brother Watch e.a.* werkt het EHRM deze waarborgen verder uit in de context van het Britse systeem van bulkinterceptie. Daarbij is voor dit rapport in het bijzonder de overweging relevant dat de autorisatie voor bulkinterceptie vooraf moet worden gegeven door een instantie die onafhankelijk is van de uitvoerende macht, niet noodzakelijk een rechter. Het autorisatieorgaan moet worden geïnformeerd over de doelstellingen van de interceptie en de verwachte communicatieroutes ('fibers' of kanalen) die zullen worden geïntercepteerd. Op die manier kan het autorisatieorgaan de noodzakelijkheid en proportionaliteit van de bulkinterceptie beoordelen en bekijken of de juiste keuzes zijn gemaakt. Voor wat betreft de toepassing van selectiecriteria of zoektermen – in de tweede fase waarin het (geautomatiseerd) doorzoeken van de geïntercepteerde gegevens plaatsvindt – vindt het Hof het niet nodig dat deze allemaal worden vermeld in het toestemmingsverzoek. De inbreuk is in deze fase minder groot dan de fase waarop inhoudelijk onderzoek van de gegevens plaatsvindt. In het Britse systeem moet voorafgaand een intern toestemmingsproces plaatsvinden en moet er per geval,

[11] *Big Brother Watch e.a.,* par. 323.
[12] *Big Brother Watch e.a.,* par. 446.
[13] *Big Brother Watch e.a*., par. 339 met verwijzing naar *Klass e.a*., par. 49, 50 en 59; *Roman Zakharov*, par. 232; *Weber en Saravia*, par. 106 en *Kennedy,* par. 153 en 154.
[14] *Big Brother Watch e.a*., par. 350. Het EHRM verwijst daarbij ook expliciet naar het rapport van de 'Venice Commission', die tevens concludeert dat de twee belangrijkste waarborgen bij bulkinterceptie bestaan uit een systeem van autorisatie en onafhankelijk toezicht op het gehele proces.

objectief worden geverifieerd of de rechtvaardiging voor het toepassen van selectiecriteria voldoet aan de vereisten.[15]

Ieder stadium van het bulkinterceptieproces moet onderhevig zijn aan toezicht door een onafhankelijke autoriteit. Inlichtingendiensten moeten zorgvuldig documenteren wat er in de verschillende stadia van het proces gebeurt, zodat een toezichthouder dit kan controleren.[16]

Ten slotte moet er een 'effectief rechtsmiddel' beschikbaar zijn voor eenieder die het vermoeden heeft dat zijn communicatie is verwerkt door de inlichtingendiensten, hetzij om de wettigheid van de interceptie aan te vechten, hetzij om de verenigbaarheid van het regime met het EVRM als zodanig te betwisten.[17] Of een rechtsmiddel effectief is, wordt bepaald aan de hand van de bevoegdheden van de bevoegde autoriteit en de geboden procedurele waarborgen. Het orgaan die de verzoeken van betrokkenen behandeld hoeft geen rechterlijke instantie te zijn. Van belang is dat het orgaan onafhankelijk is van de uitvoerende macht en een eerlijke – en zoveel als mogelijk een op tegenspraak gerichte – procedure garandeert. De oordelen moeten gemotiveerd én juridisch bindend zijn, onder meer met betrekking tot de beëindiging van onrechtmatige interceptie en het vernietigen van onrechtmatig verkregen of opgeslagen gegevens.[18] Paragraaf 2.1.3 zet deze vereisten voor een 'effectief rechtsmiddel' op basis van andere jurisprudentie van het EHRM verder uiteen.

*Acties Verenigd Koninkrijk na Big Brother Watch e.a.*

Het EHRM veroordeelde het Verenigd Koninkrijk onder andere voor een schending van artikel 8 EVRM, vanwege tekortkomingen in de voorafgaande autorisatie voor bulkinterceptie onder de (oude) RIPA.[19] Het Verenigd Koninkrijk ondernam daarop actie.

Mede naar aanleiding van deze uitspraak is in september 2017 is de '*Investigatory Powers Commissioner's Office'* (hierna: IPCO) opgericht. Deze onafhankelijke instantie houdt toezicht op onderzoeksbevoegdheden van Britse inlichtingen- en veiligheidsdiensten. In paragraaf 6.3.1 wordt IPCO verder omschreven.

Het EHRM was positief over het bestaan van de *'Investigatory Powers Tribunal'* (hierna: IPT). De IPT is een speciale rechtbank die is ingesteld voor de behandeling van klachten van burgers over vermeend onrechtmatig handelen door Britse inlichtingendiensten op basis van de RIPA. Het is bevoegd de klachten te onderzoeken, van staatsgeheime informatie kennis te nemen en relevante documentatie bij de diensten op te vragen. Het IPT kan ook raadsheren benoemen om namens de klagers inbreng te leveren tijdens hoorzittingen waar zij niet vertegenwoordigd kunnen worden. Als een schending van de RIPA wordt vastgesteld, kan de IPT een schadevergoeding toewijzen en het bevel geven tot vernietiging van gegevens naar aanleiding van het onrechtmatig handelen. Het EHRM typeert de IPT als een instantie die een 'robuust rechtsmiddel' biedt.[20] In paragraaf 6.3.2 wordt verder ingegaan op het IPT.

[15] *Big Brother Watch e.a*., par. 351-355.
[16] *Big Brother Watch e.a.,* par. 356.
[17] *Big Brother Watch e.a.,* par. 356.
[18] *Big Brother Watch e.a.,* par. 359.
[19] *Big Brother Watch e.a.,* par. 425-427.
[20] *Big Brother Watch e.a.,* par. 122-127, 413 en 415.

### 2.1.2 Centrum för Rättvisa

Op 25 mei 2021 deed de Grote Kamer van het EHRM eveneens uitspraak in de zaak *Centrum för Rättvisa* tegen *Zweden*.[21] In deze zaak staat een klacht centraal van de ngo 'Centrum för Rättvisa' tegen het optreden van de Zweedse communicatie-inlichtingendienst *Försvarets radioanstalt* (FRA). Centrum för Rättvisa is een Zweedse ngo die strategisch procedeert voor mensenrechten. Net als Big Brother Watch vreesde deze ngo dat, gezien de aard van haar werkzaamheden en de ruime bevoegdheden van de Zweedse inlichtingendienst die bevoegd is tot bulkinterceptie, haar communicatie werd onderschept.

In haar uitspraak erkent het EHRM, in dezelfde bewoordingen als in de uitspraak *Big Brother Watch*, dat bulkinterceptie een belangrijk middel kan zijn om de nationale veiligheid in verdragsstaten te beschermen.[22] Het EHRM erkent ook dat dat het verzamelen van signaalinlichtingen op het gebied van 'defensie-inlichtingen' in verschillende opzichten verschillen van interceptie in het kader van strafrechtelijk onderzoek en rechtshandhaving. In tegenstelling tot interceptie in het kader van de strafrechtelijke rechtshandhaving, zijn signaalinlichtingen in de Zweedse context primair gericht op internationale communicatie en worden ze gebruikt om defensie-inlichtingen te verkrijgen.[23]

*Gedetailleerde wettelijke regeling*

Het EHRM oordeelde dat de gronden waarop bulkinterceptie kan worden ingezet duidelijk zijn gedefinieerd in de Zweedse regelgeving. Het bevat ook het noodzakelijke voorafgaande toezicht op aangevraagde machtigingen voor bulkinterceptie en voldoende *ex post facto* toezicht. Het EHRM oordeelde ook dat de Zweedse regelgeving met betrekking tot de omstandigheden waarbij de communicatie van personen kan worden geïntercepteerd voldoende duidelijk is. Het Zweedse systeem bevat over het algemeen voldoende wettelijke waarborgen om misbruik van de bevoegdheid tot bulkinterceptie te voorkomen.[24]

*Ex ante toezicht op bulkinterceptie*

In Zweden moet de rechtbank '*Försvarsunderrättelsedomstolen'* (hierna: 'Defensie Inlichtingenhof') machtigingen voor bulkinterceptie op rechtmatigheid beoordelen. Deze autoriserende instantie moet op de hoogte worden gebracht van het doel van de inlichtingenoperatie en van de signaaldragers of communicatiekanalen die naar verwachting worden gebruikt om signalen te verwerven. Het Defensie Inlichtingenhof kan daarmee de noodzaak en evenredigheid van de zoekactie beoordelen. Bovendien moet de machtiging ten minste de soorten of categorieën zoektermen vaststellen die zullen worden gebruikt. Verder moet elk gebruik van zoektermen met betrekking tot identificeerbare personen worden gerechtvaardigd door de beginselen van noodzakelijkheid en evenredigheid. Dit moet worden geregistreerd en vooraf intern worden geautoriseerd, zodat afzonderlijk en objectief kan

[21] EHRM (GK) 25 mei 2021, nr. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa t. Zweden*).
[22] *Centrum för Rättvisa e.a.*, par. 23 en par. 365. Het hiernavolgende is deels gebaseerd op p. 51-81 van het Zweedse rapport 'Tussentijds verslag van de commissie inzake de herziening van de wet op de signaalinlichtingenactiviteiten op defensiegebied' (hierna: SOU 2023).
[23] *Centrum för Rättvisa e.a.*, par. 236-237.
[24] *Centrum för Rättvisa e.a.*, par. 279-288 en par. 316.

worden gecontroleerd of de rechtvaardiging voldoet aan bovengenoemde vereisten.[25] Het EHRM acht het Zweedse Defensie Inlichtingenhof onafhankelijk van de uitvoerende macht.[26]

Hoewel het Inlichtingenhof geen openbare hoorzittingen houdt en geen openbare beslissingen neemt, houdt het EHRM er rekening mee dat een zogenoemde 'privacyfunctionaris' als de taak heeft de privacybelangen van individuen in het autorisatieproces te waarborgen.[27] Het EHRM merkte in de uitspraak verder op dat de verwerking van persoonsgegevens door de FRA wordt gereguleerd door andere regelgeving over de verwerking van persoonsgegevens. Dit voegt een extra beschermingslaag toe (naast de bestaande wettelijke bepalingen voor signaalinlichtingen). Het EHRM oordeelde dat de Zweedse wetgeving inzake de aanvragen, selectie, het onderzoek, en het gebruik van verzamelde gegevens voldoende procedurele waarborgen tegen misbruik bevat.[28]

*Ex post facto toezicht op bulkinterceptie in Zweden*

In *Big Brother Watch* en *Centrum för Rättvissa* benadrukt het EHRM dat elke fase in het proces van bulkinterceptie onder toezicht moet staan van een onafhankelijke autoriteit. Het toezicht moet voldoende robuust zijn om ervoor te zorgen dat de inmenging met het recht op privacy beperkt blijft tot wat noodzakelijk is in een democratische rechtsstaat. De toezichthoudende instantie moet de noodzaak en evenredigheid van de genomen maatregelen kunnen beoordelen in verhouding tot de inbreuk op de fundamentele rechten van de betrokkenen.[29]

In Zweden houdt de specialistische toezichthouder *Statens inspektion för försvarsunderrättelseverksamheten* (hierna: Siun) ex post toezicht op de activiteiten van defensie-inlichtingendienst en in het bijzonder op bulkinterceptie. Ook de Zweedse gegevensbeschermingsautoriteit heeft bepaalde toezichthoudende bevoegdheden met betrekking tot de verwerking van gegevens (zie verder hoofdstuk 4).

Siun wordt door het EHRM beoordeeld als een onafhankelijk toezichthoudend orgaan, mede vanwege het feit dat het Siun wordt voorgezeten door rechters (of voormalige rechters). De leden worden benoemd uit kandidaten die zijn voorgedragen door de politieke fracties en dat die leden worden benoemd door de regering, voor een termijn van minimaal vier jaar. Ook heeft Siun ruime bevoegdheden die de activiteiten van de inlichtingendienst van het begin tot het eind omvatten en heeft Siun de bindende bevoegdheid tot het vernietigen van gegevens. Van belang is ook dat de Siun de mogelijkheid heeft om de gebruikte zoektermen door de FRA te controleren en dat de Siun toegang heeft tot alle relevante documenten van de FRA. Siun heeft een verplichting om in bepaalde gevallen te rapporteren aan andere autoriteiten, die op hun beurt de bevoegdheid hebben om juridisch bindende beslissingen te nemen.[30] Ten slotte merkte het Hof op dat Siun de activiteiten van FRA actief evalueert, zowel op algemeen niveau als op verschillende thema's, dat Siun een openbaar jaarverslag publiceert, en dat de Zweedse nationale rekenkamer Siun heeft gecontroleerd.[31] Het EHRM stelde vast dat er sprake is van

[25] *Centrum för Rättvisa e.a.,* par. 295-316.
[26] *Centrum för Rättvisa e.a.,* par. 266-269.
[27] *Centrum för Rättvisa e.a.,* par. 296 en 297
[28] *Centrum för Rättvisa e.a.,* par. 316
[29] *Centrum för Rättvisa e.a.,* par. 270
[30] SOU 2023, p. 60.
[31] *Centrum för Rättvisa e.a.,* par 350-352.

effectief en onafhankelijk toezicht is op de Zweedse activiteiten op het gebied van bulkinterceptie.

Zweden werd in *Centrum för Rättvisa* door het EHRM veroordeeld tot een schending van artikel 8 EVRM vanwege: (1) het ontbreken van duidelijke regels omtrent de vernietiging van onderschepte communicatie, (2) het ontbreken van een vereiste afweging van individuele privacybelangen bij het verstrekken van gegevens aan buitenlandse partners in de nationale regelgeving, en (3) het ontbreken van effectieve controle achteraf naar aanleiding van een klacht van een individu.[32] De derde inbreuk is het belangrijkst voor dit rapport en deze wordt hieronder kort toegelicht.

*Effectief rechtsmiddel*

Volgens het EHRM moet een effectief rechtsmiddel beschikbaar zijn voor iedereen die vermoedt dat diens communicatie is onderschept door inlichtingendiensten. Een rechtsmiddel is alleen doeltreffend als het wordt uitgevoerd door een instantie die onafhankelijk is van de uitvoerende macht. Het orgaan, dat geen rechterlijke instantie hoeft te zijn, moet een eerlijke en (voor zover mogelijk) adversaire procedure waarborgen. Een beslissing van de instantie moet met redenen zijn omkleed en juridisch bindend zijn wat betreft de beëindiging van onrechtmatige interceptie en de vernietiging van onrechtmatig onderschept of opgeslagen materiaal.[33]

In Zweden heeft de specialistische toezichthouder Siun tot taak te controleren of de activiteiten van de defensie-inlichtingendienst worden uitgevoerd in overeenstemming met de Zweedse wet- en regelgeving. Bovendien moet Siun op verzoek van een persoon nagaan of de communicatie rechtmatig is verzameld en de verwerking van deze gegevens rechtmatig heeft plaatsgevonden. De betrokkene moet in kennis worden gesteld dat Siun de controles heeft uitgevoerd.[34] In de uitspraak stelt het EHRM dat het huidige Zweedse systeem aanvaardbaar is, voor zover Siun juridisch bindende besluiten neemt en de organisatie in bepaalde gevallen verplicht is verslag uit te brengen aan een bevoegde autoriteit.[35]

Echter, de tekortkoming in de Zweedse regeling van destijds, bestaat vanwege de duale rol van Siun met betrekking toezicht en het behandelen van klachten. Volgens het Hof zouden zich situaties kunnen voordoen waarin Siun bij een controle op verzoek van een particulier moet heroverwegen wat de autoriteit eerder in het kader van haar toezicht op FRA heeft geconcludeerd. Gezien de vertrouwelijkheid en het feit dat Siun geen met redenen omklede beslissingen neemt, oordeelde het Hof dat er twijfel kan ontstaan over de vraag of de toetsing door Siun van klachten van individuen in deze gevallen voldoende waarborgen biedt voor objectiviteit en nauwkeurigheid. Het EHRM was van mening dat de dubbele rol van Siun belangenconflicten kan creëren en ertoe kan leiden dat nalatigheden of onregelmatigheden over het hoofd worden gezien om kritiek te vermijden.[36]

[32] *Centrum för Rättvisa e.a*., par. 359-364.
[33] *Centrum för Rättvisa e.a.,* par. 273.
[34] SOU 2023, p. 83.
[35] SOU 2023, p. 89.
[36] *Centrum för Rättvisa e.a.,* par. 359.

*Acties Zweden na Centrum för Rättvisa*

Naar aanleiding van de veroordeling van Zweden, heeft de Zweedse regering op 29 mei 2024 een wetsvoorstel aangenomen dat de geconstateerde problemen met betrekking tot de doorgifte van gegevens aan partnerdiensten tracht op te lossen. Deze wijzigingen zijn op 1 juli 2024 in werking getreden.[37]

Daarnaast heeft de Zweedse regering ervoor gekozen een speciale behandelkamer voor klachten in te richten bij Siun om klachten van individuen te onderzoeken.[38] Het besluitvormingsorgaan – letterlijk te vertalen als 'Delegatie voor controle op verzoek van een individu' – kan bindende besluiten nemen.

Aangezien het nieuwe besluitvormingsorgaan binnen Siun is opgericht, heeft ook dit orgaan toegang tot relevante documenten die nodig zijn voor de taakuitoefening. Ambtenaren die werkzaam zijn bij het secretariaat zijn niet bevoegd om besluiten te nemen over de aangelegenheden van het besluitvormingsorgaan of over de toezichthoudende activiteiten van de commissieleden die Siun leiden. De werkzaamheden binnen het secretariaat worden zodanig georganiseerd dat mogelijke belangenconflicten worden vermeden.[39] De wijzigingen betreffende de instelling van dit nieuwe besluitvormingsorgaan binnen Siun zijn op 1 januari 2025 in werking getreden.[40] In paragraaf 4.3.2 wordt verder ingegaan op Siun.

### 2.1.3 Association Contrafraternelle de la Presse Judiciaire e.a.

In 2024 heeft het EHRM in de zaak *Association Contrafraternelle de la Presse Judiciaire e.a. t. Frankrijk* belangrijke overwegingen gewijd aan de vraag wat een 'effectief rechtsmiddel' is in de context van het Franse toezichtstelsel op de inlichtingen- en veiligheidsdiensten.[41] Ook beschrijft het EHRM het Franse toezichtstelsel op de inlichtingen- en veiligheidsdiensten. Hieronder volgt een korte beschrijving van het toezichtstelsel op basis van de uitspraak.

Het toezichtstelsel in Frankrijk berust op twee pijlers. Het toezicht wordt uitgeoefend door de specialistische toezichthouder de *Commission nationale de contrôle des techniques de renseignement* (hierna: CNCTR) en de hoogste Franse bestuursrechter, de *Conseil d'État* (vergelijkbaar met de Afdeling bestuursrecht van de Raad van State in Nederland).

De CNCTR houdt toezicht op de naleving van de bevoegdheden die Franse inlichtingen- en veiligheidsdiensten mogen inzetten. De CNCTR voert onderzoeken uit op eigen initiatief en in het kader van klachtbehandeling van een verzoeker. De CNCTR heeft voor de taakuitvoering toegang tot staatsgeheimen en bezit onderzoeksbevoegdheden die haar toegang geven tot gegevens die in het bezit zijn van de inlichtingendiensten of de CNCTR.[42] Bij geconstateerde onrechtmatigheden kan de CNCTR aanbevelingen doen aan de minister of het betrokken departement om het verzamelen van inlichtingen stop te zetten en het verzamelde materiaal te

[37] Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024.
[38] SOU 2025, p. 206.
[39] Zie Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024 met verwijzing naar p. 38 van Wetsvoorstel 2023/24:136.
[40] Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024.
[41] EHRM 10 december 2024, nrs. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15, 59621/15, 30635/17, 30636/17, ECLI:CE:ECHR:2024:1210DEC004952615 (*Association Confraternelle de la Presse Judiciare et Autres t. Frankrijk*).
[42] *Association Confraternelle de la Presse Judiciare e.a.*, par. 116.

vernietigen. Indien de CNCTR van mening is dat het gevolg dat aan zijn aanbeveling wordt gegeven onbevredigend is, kan de CNCTR de zaak voorleggen aan de Conseil d'État.[43]

De Conseil d'État kan een klacht als beroepsinstantie voorgelegd krijgen door eenieder over vermeend onrechtmatig handelen (een klacht), nadat een klacht is behandeld door de CNCTR. Zoals hierboven is omschreven, kan de Conseil d'État ook een zaak voorgelegd krijgen via de CNCTR bij het niet-opvolgen aanbeveling in het kader van toezicht. Wanneer de Conseil d'État vaststelt dat een bevoegdheid voor het vergaren van inlichtingen onrechtmatig is ingezet of dat inlichtingen onrechtmatig zijn verwerkt, dan kan het een bevel geven tot het intrekken van de machtiging voor de inzet van een bevoegdheid of de vernietiging van onrechtmatig verwerkte gegevens bevelen. Zonder staatsgeheime informatie bekend te maken, stelt de Conseil d'État in geval van een klachtzaak de verzoeker over het oordeel in kennis. Als daarom wordt verzocht, kan de verzoeker een schadevergoeding worden toegewezen.[44]

*Aanleiding*

De verzoekers stelden dat de Franse inlichtingenwet van 24 juli 2015, de *Code de la sécurité intérieure*, in strijd was met de artikelen 8, 10 en 13 EVRM. Ten eerste stelden zij dat - gezien hun beroepen in de journalistiek en advocatuur en hun werkzaamheden en betrokkenheid bij zaken die verband houden met criminaliteit, terrorisme, en inlichtingendiensten - zij een bijzonder risico liepen slachtoffer te worden van het gebruik van inlichtingenmiddelen door de Franse inlichtingen- en veiligheidsdiensten.[45] Ten tweede stelden zij dat de regeling voor de inzet van bevoegdheden jegens journalisten en advocaten onvoldoende waarborgen ter bescherming van artikel 8 en 10 EVRM zou bieden. Zij stelden dat bepaalde technieken, zoals de geautomatiseerde verwerking van verbindingsgegevens over communicatie, volgens hen niet voldoende gericht werken, en de regeling voor geheimhoudergesprekken tussen advocaten en cliënten niet voldoet aan artikel 8 EVRM.[46] Ten derde zijn zij van mening dat een schending plaatsvindt van artikel 13 EVRM, omdat de Franse wetgeving geen doeltreffende rechtsmiddelen biedt aan personen die vermoeden dat zij het onderwerp zijn geweest van een inlichtingenmiddel.[47] De verzoekers stelden dat de beperkingen van hoor en wederhoor en 'equality of arms' voor de gespecialiseerde kamer van de hoogste bestuursrechter van Frankrijk, de Conseil d'État onevenredig zijn en afbreuk doen aan de doeltreffendheid van de procedure en de indiening van klachten bij de Conseil d'État gediend was om te mislukken

*Overwegingen EHRM*

Het EHRM stelt vast dat heeft de klachten met betrekking tot de artikelen 8 en 10 EVRM niet-ontvankelijk moeten worden verklaard omdat de nationale rechtsmiddelen niet zijn uitgeput, en de klachten op grond van artikel 6 en 13 EVRM niet-ontvankelijk moeten worden verklaard omdat zij kennelijk ongegrond zijn.[48] Het EHRM voert een uitgebreide toetsing uit op artikel 13 EVRM, omdat de vraag naar de doeltreffendheid van de nationale rechtsmiddelen een voorwaarde vormt voor het beoordelen van de ontvankelijkheid van de zaak.[49]

[43] *Association Confraternelle de la Presse Judiciare e.a.*, par. 38-40.
[44] *Association Confraternelle de la Presse Judiciare e.a.*, par. 41-43.
[45] *Association Confraternelle de la Presse Judiciare e.a.*, par. 71.
[46] *Association Confraternelle de la Presse Judiciare e.a.*, par. 56 en 59.
[47] *Association Confraternelle de la Presse Judiciare e.a.*, par. 86-93.
[48] *Association Confraternelle de la Presse Judiciare e.a.*, par. 126.
[49] *Association Confraternelle de la Presse Judiciare e.a.*, par. 63.

Het EHRM is overwegend positief over het Franse toezichtsysteem met betrekking tot de behandeling van klachten over inlichtingen- en veiligheidsdiensten. Het EHRM overweegt dat de CNCTR kan worden gezien als een van de uitvoerende macht onafhankelijk orgaan, mede vanwege de benoemingsprocedure voor personen die in de commissie zitting nemen en de beroepsprocedure bij de Conseil d'État.[50] Als rechterlijke instantie is ook de Conseil d'État onafhankelijk van de onafhankelijke macht.

Het EHRM is van oordeel dat de beperkingen aan een adversaire procedure - met betrekking tot het beginsel van hoor en wederhoor en processuele gelijkheid - in de Franse procedure bij de Conseil d'État worden gecompenseerd door 'solide' procedurele waarborgen.[51] De beperkingen zijn dat als staatsgeheimen in het geding zijn, de voorzitter van de gespecialiseerde leden van de Conseil d'État kan beslissen de zaak achter gesloten deuren te behandelen en de partijen afzonderlijk te horen. Ook krijgt de verzoekende partij geen toegang tot staatsgeheime informatie, maar kunnen de rechters wel deze informatie inzien.[52] De procedure bij de behandeling van een zaak zoveel mogelijk op tegenspraak en processuele gelijkheid gericht. Tijdens de hoorzitting bij een gespecialiseerde kamer van de Conseil d'État kunnen de staat en de verzoeker mondeling opmerkingen maken. Hoewel het proces van hoor en wederhoor beperkt is tot deze twee partijen, wordt de CNCTR in kennis gesteld van alle door hen ingediende verzoeken en kan de CNCTR door de Conseil d'État worden uitgenodigd schriftelijke of mondelinge opmerkingen te maken. Vervolgens ontvangt de Conseil d'État alle documenten die door de partijen zijn overgelegd. Het rechtsorgaan heeft ook eigen onderzoeksbevoegdheden en kan ook zelf documenten opvragen bij de diensten of de CNCTR.[53]

De beslissingen van het Conseil d'État openbaar, maar zijn uitspraken ontdaan van staatsgeheime informatie. Personen die een procedure voeren bij de Conseil d'État kunnen geïnformeerd worden met de mededeling dat onrechtmatig of niet-onrechtmatig is gehandeld. Daarbij krijgt een klager niet te horen of, en welke, bevoegdheden daadwerkelijk zijn ingezet (een zogenoemd beleid van "niet-bevestiging, niet-ontkenning"). Het EHRM acht dit toelaatbaar als er voldoende waarborgen in de nationale procedure staan.[54] Het EHRM erkent de motivering van deze uitspraken beperkt is. Het merkt echter op dat zij ook eerder heeft aanvaard dat dat staten een legitieme behoefte hebben om in het geheim te opereren en dat de kennisgeving over een inlichtingenmiddel het langetermijndoel van nationale veiligheid in gevaar kan brengen en kan bijdragen tot de onthulling van de werkmethoden van de inlichtingendiensten, hun interessegebieden, en eventueel zelfs de identiteit van hun agenten. Artikel 13 EVRM kan aldus niet worden uitgelegd dat het een rechtsmiddel vereist dat aan de klagers de uitvoering van een operatie openbaar wordt gemaakt.[55]

Het EHRM is van oordeel dat deze Franse wet- en regelgeving de Conseil d'État in staat stelt uitspraak te doen met volledige kennis van zaken, in het licht van alle feiten van de zaak, en zonder beperkt te zijn tot het onderzoek van de door de verzoeker aangevoerde middelen. Zij

[50] *Association Confraternelle de la Presse Judiciare e.a.*, par. 109-110 en par. 121.
[51] *Association Confraternelle de la Presse Judiciare e.a.*, par. 113 en 116.
[52] *Association Confraternelle de la Presse Judiciare e.a.*, par. 46.
[53] *Association Confraternelle de la Presse Judiciare e.a.*, par. 116.
[54] *Association Confraternelle de la Presse Judiciare e.a.*, par. 104.
[55] *Association Confraternelle de la Presse Judiciare e.a.*, par. 118. Met verwijzing naar *Big Brother Watch e.a*., par. 322 en *Centrum för Rättvisa,* par. 236) en *Klass e.a./Duitsland*, par. 58).

is van oordeel dat het voorgaande essentiële compenserende waarborgen vormen ten aanzien van de beperkingen van de beginselen van hoor en wederhoor en de 'equality of arms' die inherent zijn aan een systeem van geheim toezicht.[56]

## 2.2 Vereisten voor toezicht op gegevensverwerking

De vereisten voor het toezicht op gegevensverwerking afkomstig uit bulkinterceptie ter bescherming van de nationale veiligheid worden in deze paragraaf uiteengezet door de relevante bepalingen uit Conventie 108+ te bespreken.

### 2.2.1 Inleiding Conventie 108+

Op 10 oktober 2018 is het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens tot stand gekomen.[57] Dit protocol, hierna 'Conventie 108+' genoemd, moderniseert het gegevensbeschermingsverdrag 'Conventie 108' uit 1981.[58]

Het originele gegevensbeschermingsverdrag uit 1981 is zeer invloedrijk geweest, omdat dit het eerste multilaterale verdrag was op het terrein van gegevensbeschermingsrecht.[59] Ook het Europees gegevensbeschermingsrecht bouwt voort op het verdrag.[60] Conventie 108 geldt voor de gegevensverwerking in zowel de publieke als private sector. Het basisverdrag bevat algemene beginselen voor de verwerking van persoonsgegevens en verplicht verdragspartijen wettelijke maatregelen te treffen om de bescherming van persoonsgegevens te eerbiedigen. De beginselen van gegevensverwerking zijn gericht op doelbinding, proportionaliteit, juistheid, het niet langer dan noodzakelijk bewaren van gegevens, de veiligheid van gegevens, en de rechten van betrokkenen (waaronder de rechten van betrokkenen om bepaalde gegevens op te vragen, te verbeteren en te vernietigen).[61] Conventie 108 is in 2001 voorzien van een Aanvullend protocol.[62] Dit protocol verplicht verdragspartijen ertoe om één of meerdere onafhankelijke toezichthoudende autoriteiten in te stellen. In Nederland is dat de Autoriteit Persoonsgegevens.

Conventie 108+ beoogt recente jurisprudentie van het EHRM met betrekking tot gegevensbescherming te codificeren. Het neemt ook de bepalingen van het Aanvullend protocol op en zorgt ervoor dat het Conventie 108 meer in lijn met de Algemene Verordening Gegevensbescherming wordt gebracht.[63] Nederland, Zweden en het Verenigd Koninkrijk

[56] *Association Confraternelle de la Presse Judiciare e.a.*, par. 116.
[57] Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, *Trb.* 2018, 201.
[58] Het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens is in Nederland in 1988 in werking getreden (ETS nr. 108, *Trb.* 1988, 7).
[59] Jansen & Reijneveld 2021.
[60] *Kamerstukken II* 2011/12, 32761, 32, p. 9.
[61] Zie artikel 4 tot en met 8 van Conventie 108. Zie ook uitgebreid Terwange 2022 en Jansen & Reijneveld 2022.
[62] Het Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, betreffende toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens van 8 november 2001, *Trb.* 2003, 122 en 165.
[63] EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxemburg: Publications Office of the European Union 2018, p. 11-12. Zie ook Ukrow 2018; Jansen & Reijneveld 2021; en Terwange 2022.

hebben Conventie 108+ op 10 oktober 2018 ondertekend, maar niet nog geratificeerd.[64] Denemarken heeft het verdrag (nog) niet ondertekend. Alleen Frankrijk heeft het verdrag op 10 oktober 2018 ondertekend en op 27 maart 2023 geratificeerd.[65]

### 2.2.2 Betekenis van Conventie 108+ in het nationale veiligheidsdomein

Voor dit onderzoek is de belangrijkste wijziging van het protocol ten opzichte van Conventie 108 dat de verdragsbepalingen óók van toepassing zijn in het nationale veiligheidsdomein en defensie. Voorheen konden bepaalde domeinen, waaronder de nationale veiligheid en defensie, in algemene zin worden uitgesloten van de werking van het verdrag.[66]

Conventie 108+ verplicht daarnaast tot de oprichting één of meerdere instanties die toezien op de naleving van verdragsrechtelijke bepalingen. Deze toezichthouder moet beschikken over onderzoeksbevoegdheden en 'interventiebevoegdheden' (handhavingsmechanismen). Toezichthouders moeten, bij vaststelling van onrechtmatigheden, besluiten kunnen nemen (met eventueel de mogelijkheid sancties op te leggen). Op die besluiten staat de rechtsgang bij rechtbanken open, en toezichthouders moeten een jaarverslag publiceren.[67] Ook moet de toezichthoudende instantie worden geraadpleegd over relevante wet- en regelgeving (een consultatieverplichting), en dient het verzoeken en klachten van burgers in behandeling te nemen.[68] De mogelijkheid van een betrokkene om de toezichthoudende autoriteit te verzoeken een klacht te onderzoeken met betrekking tot zijn of haar rechten en vrijheden in verband met de verwerking van persoonsgegevens, helpt om het recht van een effectief rechtsmiddel te garanderen, in overeenstemming met de artikelen 9 en 12 uit Conventie 108+.[69]

Het verdrag draagt ook een aantal factoren aan die bijdragen aan de onafhankelijkheid en effectiviteit van de toezichthoudende autoriteit bij de uitoefening van haar functies. Toezichthoudende autoriteiten moeten bijvoorbeeld beschikken over de nodige infrastructuur, en ook de financiële, technische, en menselijke middelen (o.a. juristen en IT-specialisten) om snel en effectief te kunnen optreden.[70]

Met betrekking tot onafhankelijkheid van toezichthouders zijn volgens de toelichting op het verdrag de volgende overwegingen van belang:

1. de samenstelling van de autoriteit;
2. de procedure voor het benoemen van haar leden;
3. de duur van de uitoefening en de voorwaarden voor het beëindigen van hun functies;
4. de mogelijkheid voor hen om zonder onnodige beperkingen deel te nemen aan relevante vergaderingen;

[64] Nederland heeft op 23 oktober 2023 een Voorstel van Rijkswet strekkende tot parlementaire goedkeuring van Conventie 108+ bij de Tweede Kamer ingediend. In het meeste recente Kamerstuk, de nota naar aanleiding van het verslag (Kamerstukken II 2023/24, 36455, nr. 8) van 1 juli 2024 geeft de Nederlandse regering te kennen dat zij zich 'conform haar toezegging zal inspannen voor de spoedige ratificatie van het wijzigingsprotocol door het Koninkrijk'.
[65] Zie Full list - Treaty Office. Op 16 juli 2025 hadden 33 landen het verdrag geratificeerd. Het verdrag treedt in werking als 38 landen het verdrag hebben geratificeerd.
[66] Zie paragraaf 47 van de toelichting bij Conventie 108+.
[67] Zie artikel 15 Conventie 108+.
[68] Zie artikel 15 Conventie 108+ en paragraaf 125-126 van de toelichting bij Conventie 108+.
[69] Paragraaf 122 van de toelichting bij Conventie 108+.
[70] Zie paragraaf 118 van de toelichting bij Conventie 108+.

5. de optie om technische of andere deskundigen te raadplegen of externe consultaties te houden;
6. de beschikbaarheid van voldoende middelen voor de autoriteit;
7. de mogelijkheid om eigen personeel aan te nemen; en
8. het nemen van beslissingen zonder onderhevig te zijn aan externe inmenging.[71]

### 2.2.3 Uitzonderingen op de verdragsbepalingen

Verdragsstaten kunnen enkele uitzonderingen maken op de verdragsbepalingen voor zover zij betrekking hebben op de nationale veiligheid en defensie. Daarbij kunnen bijvoorbeeld de rechten van betrokkenen worden beperkt, maar slechts voor zover dat bij wet is voorzien, noodzakelijk is, en de beperkingen proportioneel zijn ten aanzien van de legitieme doelen van nationale veiligheid en defensie.[72]

Met het betrekking tot het toezicht kunnen beperkingen worden aangebracht aan de eerdere genoemd onderzoeksbevoegdheden en interventiebevoegdheden (handhavingsmechanismen) van de toezichthouder.[73] Ook deze beperkingen moeten bij wet zijn voorzien, en bovendien noodzakelijk en proportioneel zijn. Deze uitzonderingen moeten door de verdragsstaat op een 'case-by-case basis' onderzocht en getoetst worden.[74] Eventuele uitzonderingen mogen geen afbreuk doen aan de onafhankelijkheid en de effectiviteit van het toezicht.[75] In de literatuur is de kritiek geuit dat deze verdragsrechtelijke afwijkingsmogelijkheid te ruim is opgezet en dat dit tot een onterecht brede speelruimte voor verdragsstaten kan leiden.[76]

## 2.3 Integratie van de vereisten voor toezicht

Op basis van de vereisten voor bulkinterceptie uit EHRM-jurisprudentie (paragraaf 2.1) en de vereisten voor toezicht uit Conventie 108+ (paragraaf 2.2), ontstaat door een integratie van deze vereisten een samenhangend toezichtskader. Deze paragraaf bespreekt kort de vereisten van onafhankelijkheid en effectiviteit voor het toezicht, de verschillende soorten toezichthouders (gecategoriseerd als 'formele toezichthouders' en 'overige toezichthouders'), en de verschillende fasen van toezicht ten aanzien van de inzet bulkinterceptie door inlichtingen- en veiligheidsdiensten.

### 2.3.1 Onafhankelijkheid en effectiviteit

Verschillende instanties kunnen bij bulkinterceptie een toezichtsrol vervullen. Uit eerder onderzoek blijkt dat het toezicht op inlichtingen- en veiligheidsdiensten binnen de Europese Unie voor elk van deze fasen zeer verschillend geregeld.[77] Op zichzelf is dat niet problematisch, omdat het EHRM ook ten dele lidstaten de ruimte laat het toezicht zelf te regelen. Het EHRM hanteert bij de beoordeling van een toezichtstelsel van het land een

[71] Zie paragraaf 129 van de toelichting bij Conventie 108+.
[72] Paragraaf 91-93 van de toelichting bij Conventie 108+. Zie artikel 11 sub a ten aanzien van artikel 9.
[73] Zie artikel 15 lid 2 sub a-d Conventie 108+.
[74] Paragraaf 93 van de toelichting bij Conventie 108+.
[75] Artikel 11 lid 3 Conventie 108+. Zie ook Jansen & Reijneveld 2021.
[76] Zie par. 3.4.3 van de Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (geschreven door T. Wetzling & C. Dietrich), 'Report on the need for a Guidance note on Article 11 of the modernised Convention 108' (versie 11 juni 2021), Straatsburg: Directoraat Generaal Mensenrechten en Rechtstaat 2021.
[77] Zie hierover de rapporten van de European Union Agency for Fundamental Rights (hierna: Fundamental Rights Agency) van 2017 en 2023.

'holistische benadering'. Daarbij kijkt het niet zozeer naar de individuele toezichtmechanismen, maar naar de doeltreffendheid van het stelsel als geheel.[78]

Het EHRM en Conventie 108+ stellen daarbij wel als eis dat het toezicht onafhankelijk en effectief moet zijn. Onafhankelijkheid betekent dat de toezichthoudende instantie los staat van de ondertoezichtgestelden van de uitvoerende macht: de inlichtingen- en veiligheidsdiensten. Ook de benoemingsprocedure en samenstelling van de leden van de autoriteit; de mogelijkheid om technische of andere deskundigen te raadplegen en externe consultaties te houden; en het nemen van beslissingen zonder onderhevig te zijn aan externe inmenging, dragen bij aan de onafhankelijkheid van de toezichthouder.[79]

Wat effectiviteit betekent wordt niet met 'harde' criteria duidelijk gemaakt. Uit de voorgaande paragrafen en uit de literatuur komen met name de volgende factoren naar boven die bijdragen aan de effectiviteit van de toezichthoudende instantie: een noodzakelijke infrastructuur om de werkzaamheden uit te voeren, alsmede de financiële, technische en personele middelen om op te kunnen treden; de bevoegdheden om zelfstandig de benodigde gegevens en informatie te verzamelen en personeel aan te stellen; en de mogelijkheid om bindende beslissingen te kunnen nemen.[80] Bij het nemen van een besluit naar aanleiding van een klacht tot vermeend onrechtmatig handelen van de diensten, is de bevoegdheid tot het nemen van een bindende beslissing wel een 'hard' vereiste (zoals ook blijkt uit paragraaf 2.1.3).

### 2.3.2 Formele toezichthouders en overige toezichthouders

Met betrekking tot de formele toezichthouders moet met name worden gedacht aan rechterlijke instanties en specialistische toezichthouders, zoals een toezichthouder gericht op de inlichtingen- en veiligheidsdiensten of een toezichthouder die zich richt op de verwerking van persoonsgegevens.[81] Ook andere instanties kunnen een belangrijke rol vervullen in het controleren van inlichtingen- en veiligheidsdiensten. Deze instanties worden in dit onderzoek 'overige toezichthouders' genoemd. De controle door deze instanties ziet vaak op specifieke aspecten van de uitvoering inlichtingen- en veiligheidsdiensten of op specifieke taken die aan de instantie zijn toebedeeld.

Nationale Rekenkamers richten zich over het algemeen op het onderzoeken en beoordelen van de financiële verantwoording van de diensten en op de doelmatigheid in de besteding van de toebedeelde budgetten door de diensten. Het takenpakket van deze Rekenkamers is divers en verschilt per land. In sommige landen heeft de Rekenkamer slechts een controlefunctie van de bestedingen van de budgetten van inlichtingen- en veiligheidsdiensten en in andere landen controleert de Rekenkamer ook of het budget efficiënt wordt ingezet en de gewenste resultaten worden bereikt.[82]

Parlementair toezicht heeft vaak de vorm van het controleren en stellen van vragen aan de minister die verantwoordelijk is voor de ministeries waar inlichtingen- en veiligheidsdiensten

[78] Zie ook Hagens & Ryngaert 2018; Jansen & Reijneveld 2021; en de toelichting op Conventie 108+, par. 119.
[79] Zie ook, o.a., het rapport voor het Europese Parlement uit 2011, p. 117-144; Born & Wills 2012, p. 7; DCAF 2017, p. 3; en de rapportages van de Fundamental Rights Agency uit 2017 en 2023.
[80] Zie ook, o.a., EP 2011, p. 117-144; Born & Wills 2012, p. 7; DCAF 2017, p. 3; Fundamental Rights Agency 2017 en 2023.
[81] Born & Wills 2012, p. 6. De rol van de media en het maatschappelijk middenveld vallen buiten de scope van dit onderzoek (zie verder van Puyvelde 2013).
[82] Zie verder Wills in: Born & Wills 2012.

onder vallen. Parlementaire commissies spelen bijvoorbeeld een rol in de toebedeling van budgetten en kunnen de bevindingen uit jaarverslagen of rapporten van andere toezichthouders bespreken in een openbaar of in een besloten debat.[83]

De nationale ombudsman is doorgaans een onafhankelijke klachtbehandelaar die zich bezighoudt met het onderzoeken van klachten van burgers over overheidsinstanties of andere organisaties. Hierbij staat niet het *rechtmatig* handelen van de inlichtingen- en veiligheidsdiensten centraal, maar het *behoorlijk* handelen. Deze instantie kan een belangrijke of zelfs de enige rol spelen bij het bieden van een effectief rechtsmiddel aan burgers. De nationale Rekenkamers, parlementaire commissies, en ombudsmaninstanties worden in dit rapport – voor zover relevant - in elk hoofdstuk per land besproken.

### 2.3.3 Fasen van toezicht

Toezicht bij de inzet van bulkinterceptie ter bescherming van de nationale veiligheid is *in alle fasen* van de inzet noodzakelijk. Het toezicht kan aan de hand van deze fasen als volgt worden onderscheiden: vooraf (*ex ante*), tijdens (*ex durante*), en achteraf (*ex post*).[84]

*Toezicht vooraf*

Ten aanzien van het ex ante toezicht bij de inzet van bulkinterceptie is een rechtmatigheidstoets vereist van een rechter of een onafhankelijke instantie. Daarbij is de ontwikkeling te signaleren dat voorheen door het EHRM een toets door rechters werd vereist en tegenwoordig steeds vaker ook toetsing door onafhankelijke instanties mogelijk is.[85]

De concrete invulling van de toets verschilt per land en is - zoals zal blijken - sterk aan verandering onderhevig, onder andere vanwege de invloedrijke EHRM-uitspraken van *Big Brother Watch e.a.* en *Centrum För Rättvisa*.

*Toezicht tijdens*

Het ex durante toezicht kan worden omschreven als het toezicht dat plaatsvindt terwijl de inlichtingen- en veiligheidsdiensten actief bezig zijn met het verwerken van de gegevens. Het kan zien op alle fasen van het de verwerking, zoals het verzamelen, filteren, opslaan, delen, en analyseren van gegevens.[86]

Dit type toezicht - in de literatuur ook wel “continuous oversight” (doorlopend toezicht) genoemd - richt zich op het monitoren van de processen om zo inbreuken op wet- en regelgeving of onrechtmatigheden vroegtijdig te signaleren en te corrigeren.[87] Toezichthouders kunnen de uitvoering bijvoorbeeld controleren op de voorwaarden die in de voorafgaande toestemming voor de uitvoering van bevoegdheden zijn gegeven, zoals bij de hackbevoegdheid

[83] Zie verder o.a., Born & Wills 2012, p. 11; Bochel & Defty 2017, p. 103; Constantino & Wagner 2024; en ten aanzien van Nederland de Graaff & Hijzen 2018.
[84] Deze fasen van toezicht zijn overigens eerder in andere rapporten van internationale organisaties gesignaleerd, zoals het *Geneva Centre for Security Sector Governance* (DCAF, 2012 en 2017) en de Fundamental Rights Agency (2023). In de modellen wordt soms de fase van ‘ex durante’ toezicht weggelaten. Tegelijkertijd wordt opgemerkt dat het toezicht doorlopend moet zijn (“continuous control”) (zie bijvoorbeeld het rapport van de Fundamental Rights Agency uit 2023, p. 12).
[85] Zie bijvoorbeeld Venice Commission 2007; Born & Wills 2012, p. 13; Weltzling & Vieth 2018.
[86] Zie, o.a., Born & Wills 2012, p. 15; Weltzling & Vieth 2018.
[87] Zie, o.a., CTIVD 2022, p. 3; Venice Commission 2007.

en bulkinterceptie.[88] Voor dit type toezicht kan het noodzakelijk om zijn directe en permanente toegang te hebben tot de systemen van inlichtingen- en veiligheidsdiensten.

Noemenswaardig is dat in Frankrijk deze toegang voor de specialistische toezichthouder - de CNCTR - wordt gefaciliteerd door een bijzondere organisatie, de '*Groupement Interministériel de Controle*' (GIC). De CNCTR voert naar eigen zeggen dagelijks online controles uit. Deze controles worden ook gebruikt ter voorbereiding van de dossiercontroles en de controles ter plaatse die de CNCTR vervolgens uitvoert in de gebouwen van de diensten.[89]

*Toezicht achteraf*

Het ex post toezicht is een vorm van toezicht die achteraf de activiteiten van inlichtingen- en veiligheidsdiensten op rechtmatigheid toetst. Het kan bijvoorbeeld zijn gericht op het vaststellen of er onrechtmatigheden in een bepaalde periode hebben plaatsgevonden bij de inzet van bevoegdheden door een inlichtingen- en veiligheidsdienst.

Veel toezichtinstanties publiceren een jaarverslag of jaarlijks rapport over hun bevindingen en activiteiten.[90] Ex post toezicht kan ook thematisch van aard zijn, waarbij een bepaald onderwerp of een specifieke bevoegdheid over een bepaalde periode wordt onderzocht. Het onderzoek vindt vaak plaats op eigen initiatief van de toezichthouder, maar kan bijvoorbeeld ook plaatsvinden op verzoek van het parlement of de diensten zelf. Ook kan onderzoek worden gedaan naar specifieke gevallen of incidenten, vaak naar aanleiding van klachten of signalen van misstanden.

Klachten over vermeend onrechtmatig of onbehoorlijk handelen door inlichtingen- en veiligheidsdiensten worden in landen door diverse instanties behandeld. Bijvoorbeeld door de rechterlijke macht, ombudsmaninstanties, of gespecialiseerde toezichthouders.[91] In paragraaf 2.1.3 is de klachtprocedure besproken in verband met het vereiste van een effectief rechtsmiddel (de 'remedy') in art. 13 EVRM.[92] Dit fundamentele recht vereist dat iedereen wiens rechten en vrijheden zijn geschonden, toegang moet hebben tot een effectief rechtsmiddel voor een nationale instantie. Zeker in het geval dat betrokkenen niet worden genotificeerd door een inlichtingen- of veiligheidsdienst over (bijvoorbeeld) de inzet van bevoegdheden, is de mogelijkheid tot het indienen van een klacht een van groot belang om te controleren of bevoegdheden rechtmatig zijn ingezet.[93] Een klacht biedt een individu de mogelijkheid om aan te geven dat die vermoedt dat diens rechten onrechtmatig zijn geschonden door de activiteiten van een inlichtingen- of veiligheidsdienst.[94] Klachten kunnen ook een aanleiding vormen nader ex post toezicht uit te voeren.

De behandeling van klachten - mogelijk nadat een klacht eerst bij de dienst zelf is ingediend - moet plaatsvinden door een onafhankelijke instantie, die daadwerkelijk de bevoegdheden heeft om na te gaan welke activiteiten tegen de betrokkene hebben plaatsgevonden.[95] Uit de

[88] CTIVD 2022.
[89] Zie Les techniques de renseignement contrôlées par la CNCTR | CNCTR (laatste geraadpleegd op 16 juli 2025).
[90] EP 2011, p. 132.
[91] Born & Wills 2012, p. 16.
[92] Zie ook Forcese in: Born & Wills 2012. Zie ook paragraaf 2.1.3.
[93] Zie FRA 2023 en par. 2.1.3 over de zaak *Association Contrafraternelle de la Presse*.
[94] Braithwaite 2006, p. 35.
[95] Zie ook Bovens & Wille 2021; Forcese in: Born & Wills 2012, p. 182; en Fundamental Rights Agency 2023, p. 27.

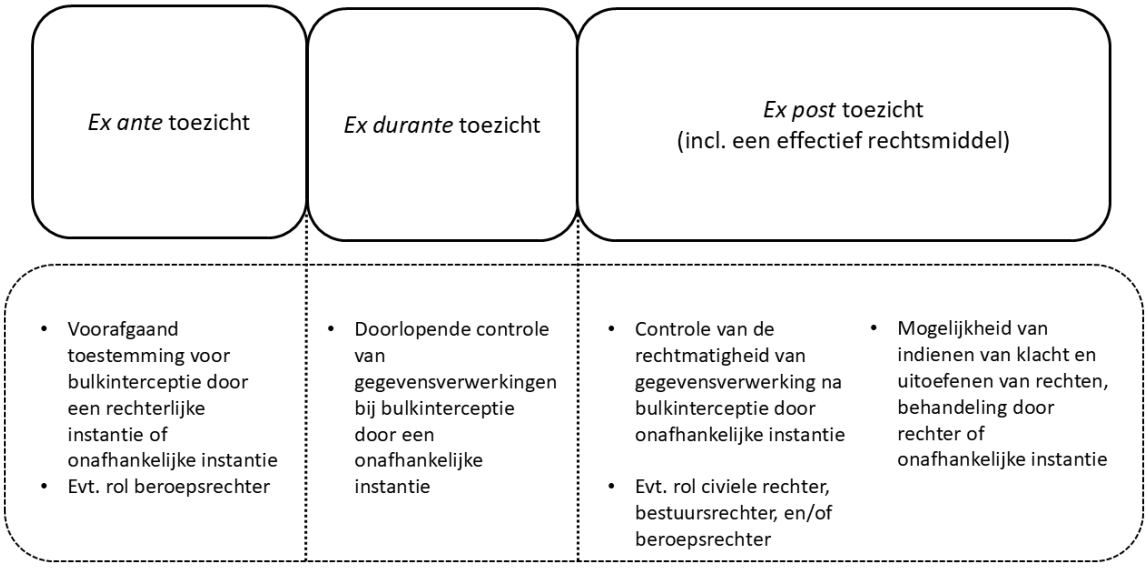
besproken EHRM-uitspraak *Association Contrafraternelle de la Presse e.a.* (in paragraaf 2.1.3), kan ook worden afgeleid dat deze instantie vervolgens ook een 'remedy' moet kunnen geven in de vorm van een bindend besluit, zoals het toekennen van een schadevergoeding voor geleden schade of het geven van de opdracht tot de vernietiging van onrechtmatige verwerkte gegevens.

Ten slotte kan het werk van inlichtingen- en veiligheidsdiensten op rechtmatigheid worden gecontroleerd door rechterlijke instanties. Daarbij gaat het vaak om gespecialiseerde rechtbanken, de bestuursrechter, of civiele rechters.

## 2.4 Conclusie

Op basis van de vereisten voor bulkinterceptie uit EHRM-jurisprudentie (paragraaf 2.1) en de bepalingen uit Conventie 108+ (paragraaf 2.2) is duidelijk dat bij de inzet van bulkinterceptie als bijzondere bevoegdheid ter bescherming van de nationale veiligheid, toezicht in alle fasen van de inzet noodzakelijk is. Zoals uit paragraaf 2.3 blijkt, kunnen verschillende instanties in elke fase van het toezicht op bulkinterceptie een toezichtsrol vervullen.

In dit rapport ligt de focus op de zogenoemde formele toezichthouders, waarbij met name worden gedacht aan rechterlijke instanties en specialistische toezichthouders. In Figuur 1 in dit rapport is uitgebeeld uit welke fasen het toezicht op bulkinterceptie bestaat en welke formele instanties daarin een rol kunnen vervullen.[96]




Figuur 1: Het stelsel van toezicht ten aanzien van bulkinterceptie

Dit toezichtsmodel laat zien welke formele toezichthouders een rol kunnen spelen in elke fase – vooraf (*ex ante),* tijdens (*ex durante*), en achteraf *(ex post*) – van bulkinterceptie. Uit de jurisprudentieanalyse van het EHRM blijkt ook dat door het EHRM de nadruk gelegd op het bestaan van een effectief rechtsmiddel (de 'remedy') in het ex post toezicht.

[96] Dit model is deels gebaseerd op een paper van Jan-Jaap Oerlemans en Mireille Hagens dat oorspronkelijk werd gepresenteerd tijdens de conferentie *'Surveillance, Democracy, and the Rule of Law'* op 9 en 10 juni 2022 aan de European University Institute in Florence.

Let op: het bovengenoemde toezichtmodel is toegespitst op bulkinterceptie en dient niet zonder meer als blauwdruk voor toezicht op andere bevoegdheden van inlichtingen- en veiligheidsdiensten. Desondanks kan de structuur van het model mogelijk ook geschikt zijn bij het toezicht op andere vergaande bevoegdheden.

Uit eerder onderzoek blijkt dat het toezicht op inlichtingen- en veiligheidsdiensten binnen de Europese Unie voor elk van de fasen zeer verschillend is geregeld. Op zichzelf is dat niet problematisch, omdat het EHRM ook ten dele lidstaten de ruimte laat het toezicht zelf te regelen. Het EHRM hanteert bij de beoordeling van het toezichtstelsel van een land een 'holistische benadering'. Daarbij kijkt het niet zozeer naar de individuele toezichtmechanismen, maar naar de doeltreffendheid van het stelsel als geheel. Toezichthouders moeten in ieder geval onafhankelijk en effectief zijn.

Uit Conventie 108+ kunnen factoren worden afgeleid die de onafhankelijkheid en effectiviteit van een toezichthouder waarborgen. Deze factoren omvatten de benoemingsprocedure en samenstelling van de toezichthoudende autoriteit, de beschikbare infrastructuur (inclusief financiële, technische en personele middelen), de bevoegdheid om zelfstandig gegevens te verzamelen en personeel aan te stellen, de mogelijkheid om deskundigen te raadplegen en externe consultaties uit te voeren, en het vermogen om beslissingen te nemen zonder onderhevig te zijn aan externe inmenging.

In hoofdstuk 3 tot en met hoofdstuk 6 wordt de precieze invulling van het toezicht uiteengezet ten aanzien van bulkinterceptie in de landen Denemarken, Zweden, Frankrijk, en het Verenigd Koninkrijk. In elk hoofdstuk wordt in de conclusie het toezichtstelsel per land in een vergelijkbaar model als in Figuur 1 gevisualiseerd.

# Hoofdstuk 3: Het toezichtstelsel in Denemarken

Dit hoofdstuk beschrijft het toezichtstelsel op de inlichtingen- en veiligheidsdiensten van Denemarken. Het geeft eerst een overzicht van deze diensten, inclusief het nationaal cybersecuritycentrum, en hun taken (zie paragraaf 3.1). De Deense regeling en het toezicht op bulkinterceptie wordt beschreven in paragraaf 3.2. Paragraaf 3.3 geeft vervolgens een overzicht van het stelsel van toezicht op de inlichtingen- en veiligheidsdiensten. Paragraaf 3.4 concludeert met een samenvatting van de belangrijkste kenmerken en werking van het Deense toezichtstelsel.

## 3.1 De inlichtingen- en veiligheidsdiensten van Denemarken

Deze paragraaf geeft een beschrijving van de twee Deense inlichtingen- en veiligheidsdiensten. De taken en positie van het nationaal cybersecuritycentrum, dat onderdeel is van de Deense militaire inlichtingendienst, wordt eveneens kort beschreven.

### 3.1.1 PET

De *Politiets Efterretningstjeneste* (hierna: PET) is een politieorganisatie en de binnenlandse inlichtingen- en veiligheidsdienst van Denemarken. Als politieorganisatie staat PET onder leiding van een directeur-generaal die rapporteert aan de minister van Justitie.[97] De focus van PET ligt op het voorkomen en bestrijden van terrorisme, extremisme, spionage, en andere bedreigingen voor de nationale veiligheid.[98]

De belangrijkste taken van PET omvatten:

1. Terrorismebestrijding: het voorkomen en bestrijden van terroristische activiteiten.
2. Spionagebestrijding: het identificeren en tegengaan van spionageactiviteiten die gericht zijn tegen Denemarken.
3. Bescherming van de democratie: het voorkomen van extremistische activiteiten die de democratische orde in gevaar brengen.
4. De beveiliging van personen en objecten: het beschermen van belangrijke personen en infrastructuur tegen potentiële bedreigingen.
5. Inlichtingenverzameling en -analyse: het verzamelen, analyseren en verspreiden van inlichtingen om potentiële dreigingen te identificeren en te neutraliseren.[99]

### 3.1.2 FE

*Forsvarets Efterretningstjeneste* (hierna: FE) is de militaire inlichtingendienst van Denemarken en onderdeel van het Ministerie van Defensie. De directeur van FE rapporteert aan de minister van Defensie. De dienst richt zich op het verzamelen van inlichtingen buitenlandse inlichtingen en militaire veiligheid.

FE verzamelt, analyseert en verspreidt informatie over omstandigheden die relevant zijn voor de veiligheid van Denemarken en de veiligheid van Deense militaire eenheden die op internationale missies worden ingezet. Het gaat dan bijvoorbeeld over het waarschuwen voor aanvallen op ingezette troepen in het binnen- of buitenland.[100] Naast het signaleren van

[97] Andersen e.a. 2022.
[98] Zie Security | | Danish Security and Intelligence Service (laatst geraadpleegd op 16 juli 2025).
[99] Zie Organization | | Danish Security and Intelligence Service (laatst geraadpleegd op 16 juli 2025).
[100] Efterretningstjeneste (laatst geraadpleegd op 16 juli 2025).

dreigingen voor militairen, draagt FE ook bij aan het tegengaan van cyberdreigingen tegen Denemarken en Deense belangen.[101]

FE fungeert als de SIGINT-organisatie van Denemarken.[102] Het werkt nauw samen met diverse Deense autoriteiten, zoals PET, het Centrum voor Terreuranalyse, en buitenlandse partners.[103] Als zogenoemde "all source-dienst" verzamelt FE ook informatie uit andere bronnen en combineert deze inlichtingen voor zover dat wettelijk is toegestaan. Op de website van FE worden de volgende soorten inlichtingenvergaring genoemd: *human intelligence* (HUMINT), *signals intelligence* (SIGINT), *computer network exploitation* (CNE), *geospatial intelligence* (GEOINT), *imagery intelligence* (IMINT)[104] en *open source intelligence* (OSINT).[105]

De belangrijkste taken van FE zijn:

1. Inlichtingenverzameling: het verzamelen van informatie over buitenlandse militaire en veiligheidsdreigingen.
2. Analyse en rapportage: het analyseren van de verzamelde gegevens en rapporteren aan de Deense regering en strijdkrachten.
3. Ondersteuning van militaire operaties: het bieden van inlichtingenondersteuning aan Deense militaire eenheden die internationaal zijn ingezet.
4. Cyberveiligheid: het beschermen van Denemarken tegen cyberdreigingen en aanvallen.
5. Samenwerking met bondgenoten: het samenwerken met buitenlandse inlichtingendiensten om gezamenlijke veiligheidsdoelen te bereiken.[106]

### 3.1.3 CFCS

Het Deense Cybersecuritycentrum (*Center for Cybersikkerhed* (hierna: CFCS)) heeft als belangrijkste taak het waarborgen van een hoog niveau van nationale beveiligingsinfrastructuur en daarmee een hoog niveau van ICT-beveiliging in Denemarken. CFCS is onderdeel van de militaire inlichtingendienst FE en richt zich specifiek op het tegengaan van geavanceerde cyberaanvallen tegen Deense overheidsinstanties en particuliere bedrijven die essentiële functies vervullen.[107]

CFCS werd in 2012 opgericht en heeft de volgende taken:

1. Functioneren als nationale en militaire alarmdienst (een 'Computer Emergency Response Team' (hierna: CERT) voor cyberdreigingen.
2. Functioneren als nationale IT-beveiligingsautoriteit (met uitzondering van het gebied van het ministerie van Justitie, waar PET verantwoordelijk is).
3. Functioneren als autoriteit voor informatiebeveiliging en paraatheid bij noodsituaties op het gebied van telecommunicatie.[108]

[101] Produkter og kunder (laatst geraadpleegd op 16 juli 2025).
[102] Andersen e.a. 2022.
[103] Om os en Efterretningskredsløbet (laatst geraadpleegd op 16 juli 2025).
[104] Met deze vorm van inlichtingenverzameling worden visuele gegevens geanalyseerd om informatie te verkrijgen. Deze gegevens zijn bijvoorbeeld afkomstig van satellieten, verkenningsvliegtuigen en drones.
[105] Zie Efterretningskredsløbet voor informatie over de verschillende soorten inlichtingenmethoden.
[106] Zie Om os (laatst geraadpleegd op 16 juli 2025).
[107] CFCS | TET (laatst geraadpleegd op 16 juli 2025).
[108] CFCS | TET (laatst geraadpleegd op 16 juli 2025).

De rol van CFCS als nationale IT-beveiligingsautoriteit valt buiten de reikwijdte van de Deense wetgeving voor inlichtingen- en veiligheidsdiensten. Dit wordt geregeld in de Wet betreffende het Centrum voor Cyberveiligheid (de CFCS-wet).[109]

## 3.2 De uitoefening van bulkinterceptie in Denemarken

Deze paragraaf bespreekt de Deense wetgeving voor inlichtingen- en veiligheidsdiensten met betrekking tot het bulkinterceptieregime en het toezicht daarop. Het beschrijft het Deense stelsel ten aanzien van bulkinterceptie en het toezicht ervan van 2013 tot en met 30 april 2025 (paragraaf 3.2.1). De ontwikkelingen na 1 mei 2025 zijn in dit rapport niet meegenomen. Op deze datum nog niet bekend of het nieuwe wetsvoorstel, dat het toezichtstelsel in Denemarken aanzienlijk zal veranderen, wordt aangenomen. De belangrijkste bepalingen uit het wetsvoorstel ten aanzien van het toezicht op bulkinterceptie zijn beschreven in paragraaf 3.2.2.

### 3.2.1 Bulkinterceptie en toezicht van 2013-2025

In 2013 heeft het Deense parlement wetgeving aangenomen die de militaire inlichtingendienst (FE) en de politie inlichtingen- en veiligheidsdienst PET een expliciete juridische basis gaf.[110] Deze wet verankerde voor het eerst na het democratisch proces de taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten in de Deense wet.[111]

Deze wetgeving kende een lange aanloop, door zowel een parlementaire onderzoekscommissie (de PET-commissie) als een evaluatiecommissie van het Deense ministerie van Justitie (de Pedersen-commissie). Deze voerden sinds 1998 een onderzoek uit naar de Deense inlichtingengemeenschap. De Pedersen-commissie presenteerde in 2012 een rapport van 600 pagina's, dat de basis vormde voor het wettelijk kader en de externe toezichthouder *Tilsynet med Efterretningstjenesterne* (hierna: TET), die op 1 januari 2014 haar werkzaamheden begon.[112] Volgens Andersen ontstond daarmee met “tegenzin van de diensten” en “geleidelijk en in beperkte mate” externe controle op de diensten. De taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten werden daarmee ook (pas) in 2013 in de Deense wet verankerd.[113]

De Deense inlichtingenwet bevat regels omtrent (a) de taken van de diensten, (b) het verzamelen en verwerken van gegevens, (c) de openbaarmaking van informatie, en (d) transparantie en geheimhouding van het werk van de diensten. Net als de reguliere politie beschikt PET over bijzondere bevoegdheden, zoals observatie, het doorzoeken van plaatsen, en de inzet van agenten. PET kan met een rechterlijk bevel communicatie onderscheppen via telecommunicatiebedrijven.[114] Deze bevoegdheden zijn geregeld in dezelfde wet als voor de

[109] Wet nr. 713 van 25 juni 2014.
[110] Wet nr. 602 van 12 juni 2013 betreffende de Deense inlichtingendienst voor Defensie (FE) (de Defensie inlichtingenwet) en het bijbehorende uitvoeringsbesluit.
[111] Andersen e.a. 2022. Denemarken heeft een Wet op de Deense politie-inlichtingendienst (PET) en een Wet op de Deense defensie-inlichtingendienst (FE). De activiteiten en bevoegdheid van CFCS zijn geregeld in de Wet betreffende het Centrum voor Cyberveiligheid (de CFCS-wet) van 25 juni 2014.
[112] Zie uitgebreid Andersen 2022. Wet op de Commissie voor de Inlichtingendiensten, cf. Geconsolideerde Wet nr. 937 van 26 augustus 2014.
[113] Andersen e.a. 2022.
[114] Zie The legal framework for PET | | Danish Security and Intelligence Service en Intelligence work | | Danish Security and Intelligence Service (laatst geraadpleegd op 16 juli 2025).

Deense politiediensten.[115] PET mag geen gegevens verzamelen door middel van bulkinterceptie.

De militaire en buitenlandse inlichtingendienst FE richt zich op het verzamelen van informatie over het buitenland.[116] De Defensie inlichtingenwet bevat een algemene bepaling met de mededeling dat FE informatie mag verzamelen en verkrijgen 'die van belang kunnen zijn voor de inlichtingenactiviteiten van de dienst'.[117] Dit omvat ook de bevoegdheid om gegevens te verzamelen via SIGINT. De regels over het verzamelen, verwerken en openbaar maken van gegevens zijn voor FE alleen van toepassing wanneer die gegevens betrekking hebben op personen en organisaties in Denemarken.[118] In alle andere situaties waarin de activiteiten van FE betrekking hebben op buitenlanders, zijn de activiteiten niet gereguleerd.[119] Het toezicht door TET is (vooralsnog) primair gericht op de rechtmatigheid van de verwerking van gegevens en is beperkt tot natuurlijke personen en rechtspersonen die zich in Denemarken bevinden.

Met de in hoofdstuk 2 geïdentificeerde vereisten op het toezicht op bulkinterceptie in het achterhoofd, is het duidelijk dat het Deense toezichtstelsel tekortkomingen bevat. De Deense wet- en regelgeving bevat namelijk geen gedetailleerde regeling voor de inzet bulkinterceptie als inlichtingenmiddel.[120] Evenmin is voorafgaande toestemming vereist voor het gebruik van het middel. Regels over samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten ontbreken eveneens, en de wet biedt geen effectief rechtsmiddel voor klachten van niet-Deense ingezetenen. De auteur Koch (2023) waardeerde de Deense wetgeving voor de Deense inlichtingen- en veiligheidsdiensten dan ook als "onvoldoende" en typeert de wet als 'kort en in zeer algemene en discretionaire termen beschreven'. De uitspraken *Big Brother Watch e.a.* en *Centrum För Rättvisa* (paragraaf 2.1.1-2.1.2) hebben pas na jaren tot aanpassingen in wetgeving geleid. Pas in juni 2024, is het toezicht op PET aangescherpt en zijn de bevoegdheden van TET uitgebreid.[121]

### 3.2.2 Wetsvoorstel 'Versterking van het toezicht op de Deense inlichtingendiensten'

Het wetsvoorstel 'Versterking van het toezicht op de Deense inlichtingendienst voor defensie' introduceert belangrijke veranderingen met betrekking voor de 'bulkverzameling' van gegevens voor defensiedoeleinden en het toezicht in Denemarken.[122] Het begrip 'bulkverzameling' omvat tevens de verzameling gegevens uit bulkinterceptie. Het verkrijgen van gegevens via bijvoorbeeld hackbevoegdheden en OSINT valt hier expliciet buiten.[123] In

[115] Zie Intelligence work | | Danish Security and Intelligence Service (laatst geraadpleegd op 16 juli 2025).
[116] Zie ook het Uitvoeringsbesluit nr. 1287 van 28 november 2017 van de wet op de Deense inlichtingendienst voor defensie.
[117] Zie sectie 3 van onderdeel 2 van de Deense wet op de militaire inlichtingendienst 2017.
[118] Zie uitgebreid over deze begrippen: p. 22 van de Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE) (versie van 31 januari 2025).
[119] Koch 2023, p. 12
[120] Koch 2023, p. 18.
[121] Wet nr. 666 van 11 juni 2024 tot wijziging van de wet op de Deense politie-inlichtingendienst (PET). Op deze wetgeving wordt verder niet ingegaan, omdat dit onderzoek zich richt op bulkinterceptie dat wordt uitgevoerd de dienst door FE.
[122] Wet tot wijziging van de wet op de Deense defensie-inlichtingendienst (FE), de wet op de bescherming van klokkenluiders en de wet op de commissie voor de inlichtingendiensten (Versterking van het toezicht op de Deense inlichtingendienst voor defensie) (conceptwetsvoorstel-versie van 31 januari 2025).
[123] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE), p. 31 (versie van 31 januari 2025).

Denemarken is er vanuit het maatschappelijk middenveld en vanuit de wetenschap kritiek op het wetsvoorstel ten aanzien van de uitbreiding van (bulk)bevoegdheden en gevolgen daarvan op het recht op privacy.[124]

De voorgestelde wijzigingen in het wetsvoorstel hebben betrekking op alle fasen van het toezicht ten aanzien van bulkinterceptie en de klachtenbehandeling achteraf. Voorgesteld wordt om de noodzaak en evenredigheid in elke fase van het proces te beoordelen. Als het wetsvoorstel wordt aangenomen, (a) wordt 'bulkverzameling' voortaan onderworpen aan onafhankelijke voorafgaande toestemming door een nieuw orgaan; (b) vindt doorlopend toezicht door een onafhankelijke toezichthouder (TET), en (c) vindt ook controle achteraf plaats door TET. De wet introduceert een nieuwe instantie – de 'Inlichtingenraad' - voor het ex ante toezicht en een nieuw 'College van toezicht op de inzagerechten' voor het toezicht achteraf. Deze paragraaf bespreekt alleen de wijzigingen ten aanzien van het toezicht op bulkinterceptie uit het wetsvoorstel.

*Ex ante toezicht*

De Inlichtingenraad wordt een nieuw onafhankelijk orgaan dat verantwoordelijk is voor de voorafgaande beoordeling van bulkverzameling van communicatiegegevens door FE. FE mag geen bulkinterceptie uitvoeren zonder voorafgaande toestemming van de Inlichtingenraad.[125]

In de aanvraag moet FE het doel van de bulkverzameling aangeven, dat wil zeggen op welke inlichtingenprioriteit(en) de verzameling van invloed kan zijn. FE hoeft geen verdere details te verstrekken over specifieke operaties die gepland zijn. Ook moet FE specificeren voor welke communicatiedragers, routes of media toestemming wordt aangevraagd. Tot slot dient FE in de aanvraag aan te geven welke categorieën of typen zoektermen gebruikt zullen worden als onderdeel van het selectiemechanisme. De toestemming voor bulkverzameling is maximaal 12 maanden geldig en kan met nogmaals 12 maanden worden verlengd.[126]

*Ex durante en ex post toezicht*

Als het wetsvoorstel wordt aangenomen, breidt het de taken van de specialistische Deense toezichthouder TET aanzienlijk uit. Voorheen lag de nadruk op rechtmatigheidscontroles ten aanzien van de verwerking van persoonsgegevens. In het wetsvoorstel wordt deze uitgebreid naar rechtmatigheidscontroles op de *operationele taken* van FE. Dit betekent dat TET achteraf kan controleren of FE handelt in overeenstemming met de geldende wet- en regelgeving, waaronder de Defensie-inlichtingenwet, bestuursrechtelijke voorschriften en algemene regels en beginselen van bestuursrecht, evenals de internationale verplichtingen van Denemarken (waaronder het EVRM).[127] Daaronder valt ook de controle of FE binnen de grenzen van de

[124] Zie bijvoorbeeld Jakob Sorgenfri Kjær, 'PET skal have lov til at masseovervåge danskere uden mistanke', *Politiken.dk*, 31 maart 2025. PET skal have lov til at masseovervåge danskere uden mistanke en Andreas Thorsen, 'I skriver hele tiden og vil høre om den nye PET-lov. Så her kommer historien', *zetland.dk*, 2 mei 2025, I skriver hele tiden og vil høre om den nye PET-lov. Så her kommer historien (laatst geraadpleegd op 16 juli 2025).

[125] Een uitzondering is mogelijk als 'het doel van de verzameling zou worden ondermijnt als op de toestemming moet worden gewacht'. In dergelijke gevallen kan FE zonder voorafgaande toestemming overgaan tot bulkverzameling, maar moet de zaak zo spoedig mogelijk en uiterlijk vijf werkdagen na het begin van het onderscheppen van communicatie aan de raad voorleggen ter goedkeuring.

[126] Idem, p. 32.

[127] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE), p. 36 (versie van 31 januari 2025).

machtiging van de Inlichtingenraad opereert.[128] In lijn met *Big Brother Watch* kent het wetsvoorstel ook een speciale regeling voor de omgang met vertrouwelijk journalistiek materiaal.[129]

*Ex post toezicht voor een effectief rechtsmiddel*

Als het wetsvoorstel wordt aangenomen, wordt op 1 januari 2026 een nieuw onafhankelijk College ingesteld: het 'College van toezicht op de inzagerechten' *(Nævnet for Indsigtsrettigheder*). Dit college, dat ook kan worden vertaald als het 'College voor de rechten op toegang tot informatie', is ontstaan naar aanleiding van de uitspraak in *Centrum för Rättvisa t. Zweden* (paragraaf 2.1.2).

Naar aanleiding van *Centrum för Rättvisa* achtte de Deense regering het noodzakelijk om een onafhankelijke instantie op te richten voor klachtbehandeling en deze instantie de mogelijkheid te geven om gemotiveerde en juridisch bindende besluiten te nemen over de verwerking van gegevens.[130] Op basis van een verzoek van een natuurlijke persoon of van een rechtspersoon, wonend in Denemarken, heeft dit college de taak om ervoor te zorgen dat FE geen informatie over hen onrechtmatig verwerkt. Voor natuurlijke personen en rechtspersonen die niet in Denemarken wonen, is het recht op toegang tot informatie afkomstig van bulkverzameling beperkt.[131]

Als het wetsvoorstel wordt aangenomen, verloopt de klachtenbehandeling als volgt. Na onderzoek door het secretariaat van TET neemt het college een beslissing en stuurt de verzoeker een met redenen omklede schriftelijke kennisgeving. Uit deze kennisgeving blijkt alleen of de verwerking van informatie over de betrokkene rechtmatig is geweest. Indien het college concludeert dat informatie onrechtmatig is verkregen of verwerkt, kan een juridisch bindend besluit worden genomen, waarbij FE wordt opgedragen om de verzameling van die informatie te staken en onrechtmatig verkregen informatie te verwijderen.[132] Het biedt daarmee een bindende beslissing.

Tot slot bevat het wetsvoorstel een externe klokkenluidersregeling voor de inlichtingen- en veiligheidsdiensten. De wet belegt deze taak bij TET.[133]

## 3.3 Het stelsel van toezicht

Deze paragraaf beschrijft het Deense toezichtstelsel op de inlichtingen- en veiligheidsdiensten, met een focus op de organisatie en bevoegdheden van de toezichthouders die toezien op de rechtmatigheid van bulkinterceptie. Daarnaast komt de mogelijkheid tot beroep tegen bindende

[128] Het is niet de bedoeling dat TET toetst of de interceptie zich richt op de juiste communicatiedragers, routes of media. Zie de toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 37 (versie van 31 januari 2025).
[129] Zie verder p. 62 van de toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE) (versie van 31 januari 2025).
[130] Idem, p. 52.
[131] Idem, p. 55. Met zoals eerder aangeven de beperking tot bulkinterceptie.
[132] Idem, p. 13.
[133] De Wet nr. 1436 van 29 juni 2021 betreffende de bescherming klokkenluiders (de 'Klokkenluiderswet') heeft onder meer tot doel Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 betreffende de bescherming van personen die inbreuken op het EU-recht melden (de Klokkenluidersrichtlijn) in Deens recht om te zetten.

besluiten van deze toezichthouders aan bod. Tot slot volgt een korte bespreking van de 'overige toezichthouders', waaronder de parlementaire commissies en de Deense Rekenkamer

### 3.3.1 De Inlichtingenraad

Als het wetsvoorstel van kracht gaat, zal de Inlichtingenraad worden opgericht. Deze instantie controleert of de bulkverzamelingsactiviteiten van FE in overeenstemming zijn met het wettelijke kader. Zonder voorafgaande toestemming van de Inlichtingenraad mag FE de gegevens niet verder verwerken.[134] Tegen beslissingen van de Inlichtingenraad kan geen beroep worden ingesteld bij een andere administratieve instantie, zoals een bestuursrechter.[135]

Met betrekking tot de samenstelling wordt voorgesteld dat de Inlichtingenraad bestaat uit een voorzitter en twee leden. Om de besluitvaardigheid van de raad te waarborgen in geval van ziekte of afwezigheid, wordt voor elk lid een plaatsvervanger aangesteld. De benoemingstermijn bedraagt vier jaar, met mogelijkheid tot herbenoeming voor nog eens vier jaar. De voorzitter moet jurist zijn en over relevante expertise beschikken, bijvoorbeeld op het gebied van onder andere het bestuursrecht en de bescherming van mensenrechten. Eén van de andere leden moet advocaat zijn, benoemd op aanbeveling van de Deense orde van advocaten. De overige leden moeten inzicht hebben in inlichtingen- of veiligheidsbeleidsaangelegenheden, of expertise hebben op het gebied van informatie- en communicatietechnologie. Om twijfel over de onafhankelijkheid te voorkomen, wordt vereist dat een lid gedurende de afgelopen vier jaar niet in dienst is geweest van het ministerie van Defensie of een van de inlichtingendiensten.[136]

Opmerkelijk is dat het wetsvoorstel stelt dat ervan uitgegaan wordt dat het ministerie van Defensie de 'praktische bijstand zal verlenen aan de Inlichtingenraad'.[137] Deze bijstand omvat bijvoorbeeld het bijeenroepen van vergaderingen, het verschaffen van toegang tot relevant materiaal, het doorsturen van verzoeken om aanvullend materiaal en het doorsturen van besluiten naar PET en andere toezichthoudende organen. Dit betekent dat de Inlichtingenraad geen eigen secretariaat zou krijgen. Dit roept vragen op over de onafhankelijkheid van dit nieuwe voorgestelde besluitvormingsorgaan.

### 3.3.2 TET

TET houdt toezicht op de op de politie-inlichtingendienst PET, de militaire inlichtingendienst FE, en het cybersecuritycentrum CFCS (dat onder FE ressorteert). TET houdt ook apart toezicht op de wetgeving voor het cybersecuritycentrum. TET's rechtmatigheidstoets richt zich op de verwerking van gegevens door het sensornetwerk van CFCS, waarmee Deense overheidsinstanties en particuliere bedrijven die nationaal belangrijke functies vervullen, zijn verbonden.[138] Ten slotte is TET verantwoordelijk voor de verzameling, verwerking en

[134] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE), p. 12 (versie van 31 januari 2025).
[135] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE), p. 3 (versie van 31 januari 2025).
[136] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE) (versie van 31 januari 2025, p. 29.
[137] Idem, p. 30.
[138] Jaarverslag CFCS 2023, p. 3.

bewaring van informatie over vliegtuigpassagiers (PNR). Elk jaar publiceert TET een verslag over de onderzoekresultaten met betrekking tot PET, FE, CFCS en de PNR-unit.[139]

De toezichthouder heeft vijf leden die worden benoemd door de minister van Justitie na overleg met de minister van Defensie. De voorzitter moet een rechter van het Hooggerechtshof zijn en wordt benoemd op aanbeveling van de presidenten van de Oostelijke en Westelijke Hooggerechtshoven van Denemarken. De overige vier leden worden benoemd door de Minister van Justitie, na overleg met de Minister van Defensie en op basis van gesprekken met *Kontroludvalget*, een parlementaire commissie.[140] TET beschikte in 2024 over 18 FTE, verdeeld over juridisch personeel met expertise in toezicht, mensenrechten en inlichtingenwetgeving, ICT-specialisten die het toezicht op digitale systemen en gegevensverwerking ondersteunen, en medewerkers in administratieve en ondersteunende functies.[141]

In mei 2025 hield TET nog met name toezicht met betrekking tot de gegevensverzameling en gegevensverwerking van de genoemde diensten ten aanzien van natuurlijke en rechtspersonen die in Denemarken wonen en die een gekwalificeerde band hebben met de Deense samenleving.[142] Vanwege de focus op gegevensverwerking en focus op Denemarken is de reikwijdte van het toezicht door daarmee TET aanzienlijk beperkt. TET behandelt ook verzoeken van natuurlijke of rechtspersonen (klagers) die in Denemarken wonen, die stellen dat de diensten onrechtmatig gegevens over hen hebben verwerkt.[143]

De toezichthouder kan rapporteren over de naleving van de gegevensverwerkingsbepalingen door de diensten en daarover advies afgeven. Indien een inlichtingendienst of het CFCS besluit een aanbeveling van TET niet op te volgen, moet zij de toezichthouder hiervan onmiddellijk op de hoogte stellen en de zaak voorleggen aan de betreffende minister ter beoordeling. Als de minister in uitzonderlijke gevallen besluit de aanbeveling van TET niet op te volgen, dient de regering de Deense parlementaire commissie voor de inlichtingendiensten hierover te informeren.[144]

TET heeft voor de uitvoering van zijn taken direct toegang tot de systemen van de ondertoezichtgestelde diensten (PET, FE, CFCS en het Deense contactpunt voor Passenger Name Records (PNR)). TET kan de diensten verzoeken en verplichten om meer informatie te verstrekken over feitelijke en juridische kwesties die relevant zijn voor hun toezichthoudende activiteiten.[145] Bovendien kunnen medewerkers van TET toegang verschaffen tot de fysieke locaties van deze diensten en medewerkers interviewen in het kader van hun onderzoekstaken.[146] TET maakt gebruik van diverse methoden om individuele gevallen te controleren, waaronder diepgaande controles, willekeurige en gerichte controles, documentatieonderzoek, inspecties en interviews. Veel documentatie over de methodologie en

[139] Zie Kontrol | tet.dk (laatst geraadpleegd op 16 juli 2025).
[140] Zie Om TET | tet.dk en de toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 20 (versie van 31 januari 2025).
[141] Jaarverslag TET 2024, p. 13 (laatst geraadpleegd op 16 juli 2025).
[142] Zie artikel 10 lid 1 en artikel 15 lid 1 van de Defensie inlichtingenwet.
[143] Zie Kontrol (laatst geraadpleegd op 16 juli 2025).
[144] Zie bijvoorbeeld het TET jaarverslag FE 2021, p. 2. toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 23 (versie van 31 januari 2025) en afdeling 16(3) van de Defensie inlichtingenwet.
[145] Artikel 17, lid 3 Defensie inlichtingenwet.
[146] Artikel 17, lid 1 en lid 2 Defensie inlichtingenwet

de wijze waarop TET risicogebaseerd toezicht heeft ingericht is beschikbaar op de website van de toezichthouder: tet.dk.

TET heeft herhaaldelijk gepleit voor een uitbreiding van haar rol en bevoegdheden, evenals een grondige herziening van het juridische kader dat met name FE en de relatie met TET regelt.[147] Zo stond in het jaarverslag van 2021 en 2022 bijvoorbeeld dat de toezichthouder van mening was dat toegang tot 'ruwe gegevens' uit SIGINT die door de militaire inlichtingendienst FE worden verwerkt noodzakelijk is, onder meer om te controleren of gegevens van Deense ingezetenen of personen in Denemarken worden verwerkt (wat niet is toegestaan zonder een rechtelijk bevel).[148] De dienst FE stelde dat de Deense toezichthouder TET informatie opvroeg die zij zelf als irrelevant beschouwden voor het extern toezicht. In 2023 bevestigde de minister van Defensie hierop dat het opvragen van 'ruwe gegevens' die worden verzameld uit bulkinterceptie buiten de bevoegdheden van de toezichthouder valt.[149]

Hierbij is opvallend dat in Denemarken de verantwoordelijke minister - en niet de rechter - klaarblijkelijk het laatste woord heeft over een dergelijk meningsverschil over de reikwijdte van de bevoegdheid van de toezichthouder. Wel moet het parlement worden geïnformeerd als de Deense minister van Justitie of Defensie een aanbeveling naast zich neerlegt, na het constateren van onrechtmatig handelen door TET.[150]

Het wetsvoorstel uit 2025 breidt de taakstelling en bevoegdheden van TET uit. In de toekomst zou TET ook in staat moeten zijn om de rechtmatigheid van de operationele activiteiten van militaire inlichtingendienst FE te controleren, zoals dat nu al het geval is met betrekking tot de politiedienst PET.[151] TET zou dan ook relevante leidinggevenden van de diensten kunnen vragen een mondelinge toelichting te geven op feiten die van belang zijn voor de toezichtactiviteiten waarvoor zij verantwoordelijk zijn en waarbij TET bevoegd is - tot op bepaalde hoogte - toezicht te houden op de verwerking van 'ruwe' gegevens door FE.[152] De regeling voor (indirecte) toegang tot gegevens via het nieuwe College voor de rechten op toegang tot informatie, zal gelden voor alle personen, ongeacht hun verblijfplaats, terwijl voor andere informatie het recht beperkt blijft tot personen die in Denemarken verblijven.[153]

Met betrekking tot de "toezichtsdynamiek" in Denemarken en de bevoegdheden van de toezichthouder mag het volgende niet onvermeld blijven. De Deense toezichthouder publiceerde in augustus 2020 een persbericht met daarin het bericht dat de militaire inlichtingendienst FE informatie achterhield en zelfs de toezichthouder probeerde te misleiden.[154] Een speciaal ingestelde onderzoekscommissie meldde later dat het management van FE niet onrechtmatig heeft gehandeld. Desondanks katalyseerde het aanvankelijke persbericht een reeks gebeurtenissen die culmineerden in de aanhouding en gevangenneming

[147] Andersen 2022.
[148] TET jaarverslag FE 2021, p. 6. En het TET jaarverslag 2022, p. 14.
[149] TET jaarverslag FE 2022, p. 7.
[150] Jaarverslag FE 2023, p. 41.
[151] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 36 (versie van 31 januari 2025).
[152] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 35 en p. 39 (versie van 31 januari 2025). De toegang zou niet reiken tot gegevens op 'individueel niveau'. Het is onduidelijk wat daarmee wordt bedoeld.
[153] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 59 (versie van 31 januari 2025).
[154] Ördén 2025 in: Vrist Rønn e.a. 2025.

van de directeur van de militaire inlichtingendienst, tegen wie aanklachten werden ingediend met betrekking tot de openbaarmaking van staatsgeheimen.[155] De strafzaak werd in 2024 geseponeerd en er vindt geen strafrechtelijke vervolging meer plaats.[156]

### 3.3.3 Het College van toezicht op de inzagerechten

Het wetsvoorstel uit 2025 regelt de oprichting van het College van toezicht op de inzagerechten als onderdeel van TET. Deze onafhankelijke commissie heeft dan tot taak om na een klacht te onderzoeken of FE rechtmatig gegevens over een natuurlijke persoon of rechtspersoon verwerkt en de klager daarvan op de hoogte te stellen. Indien het wetsvoorstel wordt aangenomen en van kracht wordt, neemt dit college de huidige klachtentaak van TET over.[157]

Het College functioneert in feite als een aparte afdeling binnen TET, waar onafhankelijk benoemde commissieleden beslissingen nemen over de klachten. Een aparte eenheid binnen het secretariaat van TET ondersteunt deze leden. Het voorstel voorziet in de aanstelling van een voorzitter en twee andere leden. Eén van hen is een advocaat die wordt benoemd op aanbeveling van de Deense orde van advocaten. Er wordt van uitgegaan dat de raad van de orde van advocaten kandidaten zal aanbevelen met voor de functie relevante competenties, zoals ervaring in publiekrecht of mensenrechtenwetgeving. Voorgesteld wordt dat het tweede lid een persoon is met inzicht in inlichtingen- of veiligheidsbeleidszaken. Het Ministerie van Defensie is van mening dat dergelijk inzicht en ervaring zullen bijdragen aan een evenwichtig toezicht. Dit lid mag in de laatste vier jaar niet in dienst zijn geweest van het ministerie van Defensie of een van de inlichtingendiensten.

De Deense regering heeft ervoor gekozen om geen nieuw instituut op te richten, omdat TET beschikt over de noodzakelijke fysieke, technische en ervaringsvoorwaarden voor het verwerken van staatsgeheime informatie. Op deze manier blijft de toegang tot vertrouwelijke informatie, staatsgeheime informatie en andere gevoelige gegevens over de activiteiten van FE beperkt tot een kleine kring van personen. De secretariaatseenheid rapporteert rechtstreeks aan het College en niet aan de overige commissieleden van TET.[158]

Het College van toezicht op de inzagerechten krijgt de bevoegdheid om bindende besluiten te nemen tegen FE, waaronder het bevel de verwerking van informatie te staken en gegevens te vernietigen, indien vastgesteld wordt dat FE onrechtmatig gegevens heeft verwerkt over een persoon die om indirecte toegang heeft verzocht. Tegen de beslissingen van het College kan geen beroep worden ingesteld bij een andere administratieve instantie, zoals een bestuursrechter.[159]

[155] Hartvigsen, Hartmann & Diderichsen 2025 in: Vrist Rønn e.a. 2025.
[156] Straffesagerne mod Lars Findsen og Claus Hjort Frederiksen gennemføres ikke | Anklagemyndigheden (laatst geraadpleegd op 16 juli 2025).
[157] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 59 en p. 100 (versie van 31 januari 2025).
[158] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 53-55 (versie van 31 januari 2025).
[159] Toelichting conceptwetsvoorstel van de Wet op de Deense defensie-inlichtingendienst (FE), p. 5-5 (versie van 31 januari 2025).

### 3.3.4 Overige toezichthouders

De Deense inlichtingen- en veiligheidsdiensten zijn onderworpen aan het toezicht van verschillende overheidsinstellingen. Hieronder volgt een kort overzicht van deze 'overige toezichthouders'.

*Rekenkamer*

De *Rigsrevisionen* (de Deense Nationale Rekenkamer) controleert de dienst op financieel gebied. Speciaal geautoriseerde ambtenaren van de rekenkamer voeren onderzoek uit en rapporteren jaarlijks aan parlementaire commissies.[160]

*Ombudsman*

De Deense Ombudsman heeft in de loop der jaren verschillende zaken onderzocht met betrekking tot de politie-inlichtingendienst PE. Deze zaken hadden voornamelijk betrekking tot de bescherming van persoonsgegevens. In de literatuur wordt aangegeven dat, ondanks de vergaande onderzoeksbevoegdheden en taakomschrijving van de parlementaire Ombudsman, deze nooit een significante rol heeft gespeeld in het toezicht op of de controle van PET of FE.[161]

Elke instelling in Denemarken die valt onder de jurisdictie van de Ombudsman is verplicht mee te werken aan het onderzoek en alle door de Ombudsman gevraagde documenten te verstrekken. Daarbij gelden echter drie categorieën uitzonderingen: staatsveiligheid, betrekkingen met buitenlandse mogendheden, en 'zorgen' die een gevaar vormen voor het leven van een derde. Volgens een Deense onderzoekscommissie is geen van deze uitzonderingen ooit ingeroepen tijdens het (weliswaar beperkte) toezicht op de Deense inlichtingengemeenschap door de Ombudsman.[162]

*Parlementaire Commissie Inlichtingen*

Het Deense parlement heeft een gespecialiseerde parlementaire commissie voor inlichtingendiensten (het *Kontroludvalget*), die zich uitsluitend bezighoudt met PET en FE.[163] Deze commissie werd in 1988 opgericht, met één vertegenwoordiger van elk van de vijf grootste partijen in het Deense parlement. De commissie benoemt haar eigen voorzitter. De leden zijn gebonden aan geheimhouding ten aanzien van de informatie die zij als commissieleden ontvangen.

De taken van de commissie zijn vastgelegd in de wet op de instelling van een commissie voor de inlichtingendiensten van defensie en de politie.[164] De regering moet de commissie op de hoogte houden van belangrijke kwesties op het gebied van veiligheid en buitenlandbeleid die relevant zijn voor de activiteiten van de inlichtingendiensten. Indien PET, FE of CFCS niet voldoen aan een verzoek van TET, dient de regering de commissie daarvan op de hoogte te stellen.[165] In buitengewone situaties kan de parlementaire commissie besluiten om TET te verzoeken specifieke zaken te onderzoeken.

[160] Rigsrevisionen / Folketinget (laatst geraadpleegd op 16 juli 2025).
[161] Andersen e.a. 2022.
[162] Adersen 2022.
[163] Zie Udvalget vedrørende Efterretningstjenesternes arbejde / Folketinget (laatst geraadpleegd op 16 juli 2025).
[164] Oversight | | Danish Security and Intelligence Service (laatst geraadpleegd op 16 juli 2025).
[165] Zie ook het Jaarverslag FE 2023, p. 41.

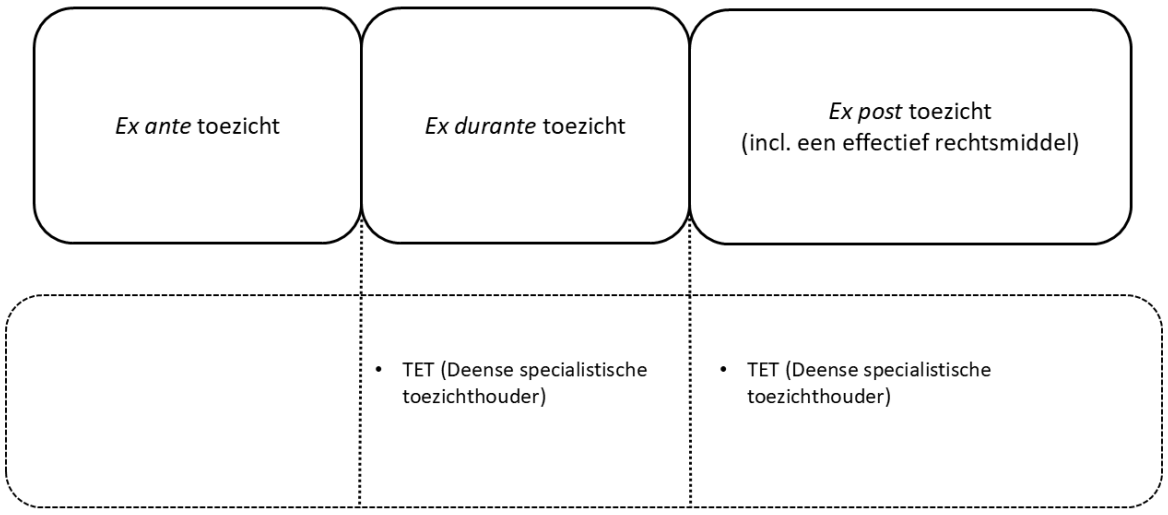
Het wetsvoorstel uit 2025 zou het mogelijk maken dat de gespecialiseerde toezichthouder TET informatie – ook staatsgeheime informatie – uitwisselt met de parlementaire commissie. Bovendien actualiseert het de regels voor de secretariaatsdiensten van de commissie.[166]

## 3.4 Conclusie

In Denemarken voert de SIGINT-dienst 'FE' bulkinterceptie uit. Deze dienst richt zich op buitenlandse dreigingen, maar houdt zich ook bezig met het tegengaan van cyberdreigingen in het binnenland en huisvest het nationaal cybersecuritycentrum van Denemarken.

Met de in hoofdstuk 2 geïdentificeerde vereisten voor toezicht op bulkinterceptie in gedachten, is duidelijk dat het huidige Deense toezichtstelsel (in mei 2025) op de inlichtingen- en veiligheidsdiensten aanzienlijke tekortkomingen vertoont. De Deense wet- en regelgeving bevat géén gedetailleerde regeling voor bulkinterceptie en de specialistische toezichthouder TET heeft geen toegang de ruwe gegevens die met SIGINT worden verzameld. Bovendien is de huidige taakstelling van TET beperkt door de focus op de rechtmatigheid van gegevensverwerkingen. De verantwoordelijke minister van een FE heeft klaarblijkelijk het laatste woord over wetsinterpretaties, hetgeen vragen oproept over onafhankelijkheid. Ten slotte valt op dat het toezicht vaak beperkt is tot particulieren en rechtspersonen die in Denemarken verblijven.

Het huidige stelsel van toezicht ten aanzien van bulkinterceptie in Denemarken is weergegeven in Figuur 2.




Figuur 2: Het stelsel van toezicht ten aanzien van bulkinterceptie in Denemarken

Het wetsvoorstel 'Versterking van het toezicht op de Deense inlichtingendienst voor defensie' uit 2025 introduceert belangrijke veranderingen met betrekking tot bulkinterceptie en het

[166] Toelichting conceptwetsvoorstel van de wet op de Deense defensie-inlichtingendienst (FE), p. 20-25 (versie van 31 januari 2025).

toezicht in Denemarken. Deze wijzigingen zijn met name ingegeven door de uitspraken van het EHRM, zoals *Centrum för Rättvisa t. Zweden* (paragraaf 2.1.2).

Als het wetsvoorstel wordt aangenomen, zal bulkinterceptie voortaan onderworpen zijn aan onafhankelijke voorafgaande toestemming door een nieuwe instantie, de 'Inlichtingenraad', vindt doorlopend toezicht plaats door de specialistische toezichthouder TET met een breder toezichtmandaat dan voorheen, en wordt het toezicht achteraf versterkt met een 'College van toezicht op de inzagerechten'.

# Hoofdstuk 4: Het toezichtstelsel in Zweden

Dit hoofdstuk beschrijft het toezichtstelsel op de inlichtingen- en veiligheidsdiensten van Zweden. Paragraaf 4.1 geeft overzicht van deze diensten, inclusief hun specifieke taken. De wet- en regelgeving en het toezicht op bulkinterceptie worden beschreven in paragraaf 4.2. Paragraaf 4.3 geeft vervolgens een overzicht van het algemene stelsel van toezicht op deze diensten. Paragraaf 4.4 biedt een samenvatting van de belangrijkste kenmerken en werking van het toezichtstelsel in Zweden.

## 4.1 De inlichtingen- en veiligheidsdiensten van Zweden

In deze paragraaf volgt een beschrijving van de inlichtingen- en veiligheidsdiensten van Zweden, d.w.z. de Zweedse (binnenlandse) veiligheidsdienst, de militaire inlichtingendienst, en de communicatie-inlichtingendienst. Daarnaast worden de taken en positionering van het Zweedse nationaal cybersecuritycentrum besproken.

### 4.1.1 SÄPO

De *Säkerhetspolisen* (hierna: SÄPO) is de Zweedse binnenlandse veiligheidsdienst en politie-inlichtingendienst. De dienst heeft zowel de taak om inlichtingen te vergaren ter bescherming van de nationale veiligheid, als een (strafrechtelijke) opsporingstaak. Deze dienst valt onder het Zweedse Ministerie van Justitie.

De taken van SÄPO zijn als volgt:

1. Contraspionage: het voorkomen en detecteren van spionage en andere illegale inlichtingenactiviteiten die gericht zijn tegen Zweden en zijn nationale belangen.
2. Contraterrorisme: het voorkomen en bestrijden van terrorisme.
3. Bescherming van hoogwaardigheidsbeklederS: de beveiliging van de leden van de Koninklijke familie, parlementsleden en ministers.
4. Contra-ondermijning: het voorkomen van intimidatie, bedreigingen, geweld, dwang of corruptie die gericht zijn op het beïnvloeden van de functies van het democratische staatsbestel. De focus ligt daarbij op politiek gemotiveerde groepen en individuen, zoals politieke en religieuze extremisten, die ernstige of systematisch uitgevoerde misdrijven plegen om de samenleving te veranderen.
5. Beveiliging: het beschermen van informatie en activiteiten die van belang zijn voor de veiligheid van Zweden tegen onder andere spionage, sabotage en terroristische misdrijven. Als onderdeel van deze taak voert het ook veiligheidsonderzoeken uit (voordat een persoon kan deelnemen aan veiligheidsgevoelige werkzaamheden).
6. Contraproliferatie: het tegengaan van programma's van massavernietigingswapens van andere landen. Het doel is om te voorkomen dat Zweedse bedrijven en onderzoeksinstituten bewust of onbewust bijdragen aan de programma's van massavernietigingswapens van andere landen.[167]

[167] Deze informatie is afkomstig van Säkerhetspolisen - Säkerhetspolisen (laatst geraadpleegd op 16 juli 2025).

### 4.1.2 MUST

De *Militära underrättelse- och säkerhetstjänsten* (hierna: MUST) is Zweedse militaire inlichtingen- en veiligheidsdienst. De dienst is verantwoordelijk voor buitenlandse inlichtingen en militaire veiligheid. Het valt onder het de natuurlijk plek van het Ministerie van Defensie. MUST maakt deel uit van de Zweedse strijdkrachten.[168] De dienst heeft ook een cyber security taak en monitort internetverkeer om de vitale infrastructuur te beschermen met zowel offensieve als defensieve maatregelen.[169]

### 4.1.3 FRA

De *Försvarets radioanstalt* (hierna: FRA) is de Zweedse communicatie-inlichtingendienst en nationale SIGINT-autoriteit. De FRA werd in 1942 opgericht en is onderdeel van het Ministerie van Defensie.[170] De FRA verzamelt gegevens door het onderscheppen van radiosignalen, satellietverkeer en internetverkeer. Andere aspecten van signaalinlichtingen zijn gericht op het vaststellen van technische details, met name radarsignalen van schepen of vliegtuigen. De defensie-inlichtingenactiviteiten van de FRA zijn met name gericht op het zoeken van nog onbekende dreigingsactoren en -verschijnselen.[171] De FRA houdt zich ook bezig met de ontwikkeling van interceptie, de nationale behoeften voor cryptografie, en de ontwikkeling systemen voor de verwerking van de gegevens via signaalinformatiesystemen.[172]

De FRA levert inlichtingen aan de Zweedse regering, de Zweedse strijdkrachten, de Zweedse veiligheidsdiensten en de Zweedse politie. De Zweedse 'Wet op de signaalinlichtingen' bevat een lijst van doelen waarvoor het in kaart brengen door middel van signaalinlichtingen bij militaire-inlichtingenactiviteiten mag plaatsvinden, zoals het in kaart brengen van externe militaire dreigingen voor het land of dreigingen voor Zweedse belangen bij de uitvoering van internationale operaties. De inlichtingenactiviteiten kunnen echter ook gericht zijn op zaken die geheel of gedeeltelijk verband houden met de activiteiten van de Zweedse veiligheidsdienst (SÄPO), zoals het in kaart brengen van strategische omstandigheden met betrekking tot internationaal terrorisme of buitenlandse inlichtingenactiviteiten tegen Zweedse belangen. SÄPO is dan ook een van de autoriteiten die kunnen beslissen over de focus van de signaalinlichtingen door de FRA. Kabelinterceptie, die alleen door de FRA uitvoert, mag alleen betrekking hebben op signalen die over de grens van Zweden worden verzonden.[173]

De regering stelt het zwaartepunt de inlichtingenactiviteiten op defensiegebied vast. De inlichtingenrapporten van de FRA mogen alleen persoonsgegevens bevatten die relevant zijn voor defensie-inlichtingenactiviteiten. Volgens Klamberg hebben deze gegevens betrekking op de volgende activiteiten: (a) externe militaire dreigingen, (b) buitenlandse inlichtingenactiviteiten tegen Zweedse belangen, (c) de Zweedse deelname aan internationale operaties, (d) internationale terrorisme en andere ernstige grensoverschrijdende criminaliteit die essentiële nationale belangen kan bedreigen, (e) de ontwikkeling en verspreiding van

[168] Deze informatie is afkomstig van The Intelligence and Security Service - Swedish Armed Forces (laatst geraadpleegd op 16 juli 2025). Zie ook SOU 2025, p. 189.
[169] Zie Cyber defence - Swedish Armed Forces (laatst geraadpleegd op 16 juli 2025).
[170] Deze beschrijving is deels afkomstig van de website van de FRA: English - FRA (laatst geraadpleegd op 16 juli 2025). Zie ook SOU 2025, p. 188.
[171] SOU 2025, p. 291.
[172] SOU 2023, p. 30
[173] SOU 2025, p. 191 met verwijzing naar artikel 2 van de Wet op de signaalinlichtingen.

massavernietigingswapens, (f) dreigingen tegen technische infrastructuren, en (g) internationale conflicten.[174] De FRA houdt zich tegenwoordig ook bezig met de detectie en tegenmaatregelen tegen cyberaanvallen gericht op de kritieke nationale IT-infrastructuur van Zweden.[175]

### 4.1.4 Nationaal cybersecuritycentrum

De FRA, MUST, het Zweedse agentschap voor civiele noodsituaties (*Myndigheten församhällsskydd och beredskap* (hierna: MSB)) en SÄPO hebben gezamenlijk een nationaal cybersecuritycentrum opgericht. Het cybersecuritycentrum heeft tot doel het nationale vermogen te vergroten om cyberaanvallen en andere IT-incidenten die de veiligheid van Zweden in gevaar kunnen brengen, te voorkomen, op te sporen en aan te pakken.[176] Voor zover bekend bestaat er geen onderliggende wet- en regelgeving voor dit centrum.

## 4.2 De uitoefening van bulkinterceptie in Zweden

Deze paragraaf begint met een beschrijving van de ontwikkeling van het juridisch kader voor bulkinterceptie in Zweden. Vervolgens wordt het ex ante toestemmingsproces besproken, waarna het ex post toezicht ten aanzien van het bulkinterceptieproces wordt behandeld.

### 4.2.1 Ontwikkeling juridisch kader voor bulkinterceptie

De FRA houdt zich sinds 1942 bezig met signals intelligence. Sinds 2009, na de inwerkingtreding van de Wet op signaalinlichtingen bij defensie-inlichtingen, voert de FRA ook kabelinterceptie uit.[177] Voor 2009 was signals intelligence niet als inlichtingenactiviteit gereguleerd, gebaseerd op het principe dat “de ether vrij is”.[178]

De Wet op signaalinlichtingen van 2009 bevat een grondslag voor de FRA om bulkinterceptie uit te voeren, voor de daaropvolgende gegevensverwerking, en het bevat een autorisatieprocedure voorafgaand aan de inzet van het middel.[179] Met de inwerkingtreding van een nieuwe wet in 2013 kreeg ook de SÄPO en de Zweedse Nationale Recherche onder bepaalde voorwaarden toegang tot de signaalinlichtingen van de FRA.[180]

Op 2 september 2024 diende de Zweedse regering een wetsvoorstel dat ruimere bevoegdheden voor bulkinterceptie mogelijk zou maken. De wijzigingen zouden de FRA een breder mandaat geven om bulkinterceptie uit te voeren in tijden van oorlog of dreiging van oorlog, een taak toewijzen aan de FRA voor het verzamelen van inlichtingen over buitenlandse investeringen,

---

[174] Klamberg 2009, p. 524.
[175] Wallin 2018, p. 25.
[176] Zie Nationellt center för cybersäkerhet (NCSC) | MSB (laatst geraadpleegd op 16 juli 2025).
[177] Zie ook Hansén 2023, p. 944.
[178] Meer precies is de verzameling en verwerking van gegevens uit signals intelligence zijn Zweden geregeld door de ‘Wet op de radio-inlichtingendienst bij activiteiten op het gebied van radio-inlichtingendienst’ (hierna: de
Wet op de radio-inlichtingendienst genoemd) van 2001, de Verordening betreffende activiteiten op het gebied van radio-inlichtingendienst bij defensie van 2000, de Verordening betreffende activiteiten op het gebied van radio-inlichtingendienst bij activiteiten op het gebied van radio-inlichtingendienst bij defensie van 2008, en de wet inzake de verwerking van persoonsgegevens door het Zweedse nationale radio-inlichtingendienst voor defensie (FRA-PuL) van 2021. Zie SOU 2023, p. 29
[179] SOU 2023, p. 27. De Zweedse Wet op de signaalinlichtingen bij defensie-inlichtingenactiviteiten is op 1 januari 2009 in werking getreden.
[180] SOU 2023, p. 29. De commissie verwijst naar het wetsvoorstel Toegang politie tot signaalinlichtingen bij inlichtingenactiviteiten defensie van 2011. Deze wet is 1 januari 2013 in werking getreden.

en een uitzondering introduceren op het huidige verbod op het verzamelen van binnenlandse communicatie.[181]

### 4.2.2 Ex ante autorisatie

De voorafgaande autorisatie wordt vanaf 2009 uitgevoerd door een gespecialiseerde rechtbank, de *Försvarsunderrättelsedomstolen*, hierna 'Defensie Inlichtingenhof' genoemd.[182] De FRA moet een aanvraag indienen voor het onderscheppen van de signalen. De aanvraag moet onder meer informatie bevatten over de missie voor het verzamelen van inlichtingen waarop de aanvraag betrekking heeft, met een gedetailleerde beschrijving van de noodzaak die aanleiding geeft tot de aanvraag en informatie over het doel van de missie, welke signaaldrager(s) de aanvraag betreft, de zoektermen of categorieën zoektermen die men wil gebruiken en de periode waarvoor de machtiging geldt. De machtiging kan worden verleend voor ten hoogste zes maanden na de datum van het besluit en kan, na hernieuwde toetsing, telkens met ten hoogste zes maanden worden verlengd.[183]

De aanvraag voor toestemming wordt door het Defensie Inlichtingenhof behandeld tijdens een hoorzitting, die over het algemeen niet openbaar is. Vertegenwoordigers van de FRA en een privacyfunctionaris zijn aanwezig bij de hoorzitting voor de rechtbank. De privacyfunctionaris is over het algemeen verantwoordelijk voor het beschermen van de privacybelangen van personen en heeft het recht om kennis te nemen van de zaak en zijn mening te geven. Deze functionaris wordt door de regering aangesteld voor telkens minstens vier jaar en moet Zweeds staatsburger zijn en advocaat zijn of zijn geweest, of een gewone rechter zijn geweest.[184]

Er kan geen beroep worden ingesteld tegen de beslissingen van het Defensie Inlichtingenhof.[185]

### 4.2.3 Ex post toezicht

De FRA kan grote hoeveelheden communicatiegegevens verzamelen en analyseren. Daarvan kunnen de zogenoemde verkeersgegevens worden gebruikt om communicatiepatronen in kaart te brengen, sociale netwerken vast te stellen en inzicht te krijgen in groepsstructuren.[186] Ook worden er zoektermen gebruikt bij het verzamelen van signalen en bij het zoeken in datasets. Deze selectiecriteria kunnen zowel persoonsgegevens (zoals een naam of taal) als technische kenmerken (zoals een e-mailadres of telefoonnummer) omvatten.[187]

De *Statens inspektion för försvarsunderrättelseverksamheten* (Siun) is de Zweedse Defensie inspectiedienst die verantwoordelijk is voor het controleren van de signaalinlichtingenactiviteiten van de FRA. Siun controleert of de FRA de wet- en regelgeving naleeft en controleert tevens de machtigingen voor signaalinlichtingen. Als bij een controle blijkt dat het verzamelen niet in overeenstemming is met de door het Inlichtingenhof verleende machtiging, kan Siun besluiten dat bepaalde verwerkingen worden gestaakt en gegevens voor

[181] Communicatie van Centrum for Rattvisa van 4 september 2024 aan de Raad van Europa naar aanleiding van de uitspraken inzake *Centrum för Rättvisa t. Zweden*.
[182] SOU 2023, p. 28.
[183] SOU 2023, p. 39 met verwijzing naar artikel 4a van de Wet op de radio-inlichtingen.
[184] SOU 2023, p. 38.
[185] SOU 2023, p. 40.
[186] Klamberg 2009, p. 520.
[187] Klamberg 2009, p. 529

zover nodig worden vernietigd. Siun controleert ook de verwerking van persoonsgegevens door MUST.[188]

Voor de FRA gelden specifieke regels met betrekking tot de verwerking van gegevens uit signaalinlichtingen. Zo moeten gegevens worden vernietigd als de gegevens niet relevant worden geacht voor defensie-inlichtingen, als deze gaan over communicatie van verschoningsgerechtigden, of signalenverkeer betreft tussen een zender en ontvanger die zich allebei in Zweden bevinden.[189] Naar aanleiding van de uitspraak in *Centrum för Rättvisa t. Zweden* voert de FRA ook een evenredigheidsbeoordeling uit, waarbij de mogelijke inbreuk op de privacy van de betrokkene wordt afgewogen tegen de inlichtingenbelangen bij de doorgifte van gegevens aan buitenlandse inlichtingen- en veiligheidsdiensten. In 2025 is een wetsvoorstel ingediend die dit expliciet in de wet moet regelen.[190] Overigens kennen MUST en FRA op heden geen maximale verwerkingstijd van gegevens. In plaats daarvan passen zij het beginsel toe dat persoonsgegevens niet langer mogen worden verwerkt dan noodzakelijk is met het oog op de doeleinden van de verwerking.[191]

Afgezien van een besluit over de vernietiging van gegevens die door de FRA zijn verzameld in strijd met de machtiging voor signaalinlichtingen, heeft de toezichthouder geen bevoegdheden om bindende beslissingen te nemen of correcties te bevelen. Siun is echter wel verplicht om omstandigheden die strafbare feiten kunnen vormen en fouten die kunnen leiden tot aansprakelijkheid voor schade voor de staat, te melden aan de Kanselier van Justitie.[192]

De wet op signaalinlichtingen bij defensie-inlichtingen bevat ook een verplichting voor Siun om op verzoek van een individu te onderzoeken of de gegevens over deze persoon rechtmatig zijn verzameld en verwerkt. Na de veroordeling van Zweden in *Centrum för Rättvisa*, heeft de Zweedse regering ervoor gekozen een speciale behandelkamer voor klachten in te richten bij Siun om klachten van individuen te onderzoeken (zie verder paragraaf 4.3.2).[193]

De Zweedse Autoriteit Persoonsgegevens - *Integritetsskyddsmyndigheten* (IMY) - houdt eveneens toezicht op de gegevensverwerking door de FRA en de Zweedse strijdkrachten. De gegevensbeschermingsautoriteit verleent, indien gerechtvaardigd, advies en ondersteuning aan de FRA en de Zweedse strijdkrachten over hun verplichtingen met betrekking tot wetgeving. Echter, deze gegevensverwerkingsautoriteit wordt niet op de hoogte gebracht van geplande verwerkingsactiviteiten. Individuen hebben ook niet de mogelijkheid om de toezichthoudende autoriteit te verzoeken na te gaan hoe de verantwoordelijken voor de verwerking persoonsgegevens in een bepaald opzicht verwerken. Het toezicht van IMY is dus in wezen beperkt tot gevallen die op eigen initiatief plaatsvinden.[194]

[188] SOU 2023, p. 43.
[189] SOU 2025, p. 202 met verwijzing naar artikel 2a en 7 van de Wet op de Signaalinlichtingen.
[190] SOU 2025, p. 82.
[191] SOU 2025, p. 468.
[192] SOU 2025, p. 206.
[193] SOU 2025, p. 206.
[194] SOU 2025, p. 209.

## 4.3 Het stelsel van toezicht

Deze paragraaf beschrijft het algemene Zweedse toezichtstelsel op de inlichtingen- en veiligheidsdiensten, met een focus op de organisatie en bevoegdheden van de toezichthouders die toezien op de rechtmatigheid van bulkinterceptie. Daarnaast komt de mogelijkheid tot beroep tegen bindende beslissingen van deze toezichthouders aan bod. Tot slot volgt een korte bespreking van de 'overige toezichthouders', zoals de parlementaire toezichthouders en de nationale Rekenkamer.

### 4.3.1 Het Defensie Inlichtingenhof

Het Defensie Inlichtingenhof beoordeelt de aanvragen voor signaalinlichtingenactiviteiten van de FRA. Deze toetsing is reeds beschreven in paragraaf 4.2. Historisch gezien was er in Zweden een terughoudendheid om defensie-inlichtingen (militaire inlichtingen, waaronder signaalinlichtingen) te vermengen met de inlichtingen gericht op de (binnenlandse) veiligheid door SÄPO. In de loop der tijd is het mandaat voor activiteiten op het gebied van defensie-inlichtingen echter aangepast, van het in kaart brengen van "externe militaire dreigingen" naar "externe dreigingen". Dit betekent dat internationaal terrorisme en ernstige grensoverschrijdende criminaliteit met gevolgen voor het veiligheidsbeleid nu ook onder de activiteiten van defensie-inlichtingen kunnen vallen.[195]

Het Inlichtingenhof bestaat uit een voorzitter, één of ten hoogste twee vicevoorzitters en ten minste twee tot maximaal zes gespecialiseerde leden. De voorzitter en de vicevoorzitters zijn juristen met ervaring als rechter. De regering benoemt de voorzitter van het Defensie Inlichtingenhof tot vaste rechter van het hof. De vicevoorzitters en de bijzondere leden worden door de regering benoemd voor een termijn van vier jaar.[196]

De bijzondere leden beschikken over gespecialiseerde kennis die relevant is voor het werk van het hof. Het Defensie Inlichtingenhof heeft ook een speciale vertegenwoordiger voor privacyrechten (de *integritetsskyddsombud*).[197] Bij een hoorzitting zijn vertegenwoordigers van de FRA en deze 'privacyombudsman' aanwezig. De privacyombudsman is verantwoordelijk voor het beschermen van de privacybelangen van betrokkenen en heeft het recht om kennis te nemen van de zaak en zijn mening te geven. Deze functionaris wordt door de regering aangesteld voor een termijn van minstens vier jaar en moet Zweeds staatsburger zijn, evenals advocaat of rechter zijn geweest.[198]

In een wetsvoorstel uit 2025 wordt voorgesteld de taken van het Defensie Inlichtingenhof uit te breiden met betrekking tot bulkdatasets (ook uit andere bronnen dan bulkinterceptie) en te fungeren als beroepsinstantie in gevallen waarin bindende beslissingen over gegevensverwerking door toezichtsinstanties worden genomen.[199]

[195] SOU 2025, p. 620.
[196] SOU 2023, p. 39.
[197] Hansén 2023, p. 945.
[198] SOU 2023, p. 38.
[199] SOU 2025, p. 705-707.

### 4.3.2 Siun

Siun is een Zweedse specialistische toezichthouder die verantwoordelijk is voor het toezicht op de activiteiten van inlichtingendiensten op defensiegebied, de naleving van de 'Wet op de signaal-inlichtingenactiviteiten' door de FRA.[200]

Siun wordt geleid door een commissie waarvan de leden door de regering worden benoemd voor een vaste termijn van minstens vier jaar. De voorzitter en de vicevoorzitter moeten gewone rechters zijn geweest, terwijl de overige leden worden voorgedragen door de fracties in het Zweedse parlement (de 'Riksdag'). De raad mag maximaal zeven leden tellen.[201] Zij worden bijgestaan door een secretariaat van onbekende grootte.[202] Siun moet elk jaar voor 1 maart een jaarverslag over de toetsingsactiviteiten bij de regering indienen.

Als bij een controle blijkt dat het verzamelen niet in overeenstemming is met de machtiging die door het Inlichtingenhof is verleend, kan Siun besluiten bepaalde verwerkingen te staken en gegevens voor zover nodig te vernietigen.[203] De NGO Centrum för Rättvisa heeft kritiek geuit op het feit dat Siun alleen gegevens mag vernietigen als de verzameling niet verenigbaar is met de toestemming van het Zweedse Inlichtingenhof, en verder niet bevoegd is om juridisch bindende besluiten te nemen. Ook kan de inspectie signalen van onrechtmatige gegevensverzameling doorgeven aan de Zweedse Autoriteit Persoonsgegevens (IMY), maar deze autoriteit heeft beperkte mogelijkheden tot actie.[204]

Naar aanleiding van de veroordeling in *Centrum för Rättvisa t. Zweden* heeft de Zweedse regering op 29 mei 2024 een wetsvoorstel aangenomen dat de geconstateerde problemen met betrekking tot de doorgifte van gegevens aan partnerdiensten moest oplossen. De wijzigingen betreffende de vernietiging van onderschept materiaal zonder persoonsgegevens en de voorwaarden voor doorgifte van persoonsgegevens aan buitenlandse ontvangers zijn op 1 juli 2024 in werking getreden.[205]

Zoals beschreven in paragraaf 4.2.2, moet Siun op verzoek van een individu ook onderzoeken of de gegevens uit signaalinlichtingen rechtmatig zijn verwerkt. In de zaak *Centrum för Rättvisa t. Zweden* oordeelde het EHRM dat de duale taak van Siun – het toezicht houden op activiteiten van inlichtingendiensten op defensiegebied en optreden als klachtbehandelaar, gecombineerd met het feit dat een persoon geen gemotiveerde beslissing ontvangt na een klacht – resulteert in een gebrek aan effectieve controle achteraf.[206]

Zoals in paragraaf 2.1.2 al is genoemd, heeft de Zweedse regering in reactie daarop de wet aangepast en een besluitvormingsorgaan binnen Siun voor de klachtbehandeling ingesteld. De overwegingen om niet een geheel nieuwe autoriteit op te richten waren destijds dat er slechts een beperkt aantal verzoeken per jaar beoordeeld hoefde te worden en dat een kleine organisatie kwetsbaar is voor personeelsverloop, wat kan leiden tot verlies van kennis op het gebied van

[200] SOU 2023, p. 43.
[201] SOU 2023, p. 43. De commissie verwijst naar artikel 8 en artikel 10 van de van de verordening met instructies voor de FRA.
[202] SOU 2023, p. 11.
[203] SOU 2023, p. 43.
[204] Zie de Communicatie van Centrum for Rättvisa naar aanleiding van de zaak Centrum för rättvisa t. Zweden van 4 september 2024.
[205] Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024.
[206] Centrum för Rättvisa e.a., par. 369.

inlichtingen. Aangezien relevante en voldoende kennis noodzakelijk is om de controle uit te voeren, zouden dit uiteindelijk negatieve gevolgen kunnen hebben, zoals onjuiste controles of onnodige vertragingen.[207]

Het besluitvormingsorgaan – letterlijk te vertalen als 'Delegatie voor controle op verzoek van een individu' – bestaat uit een voorzitter, een vicevoorzitter (die ervaring hebben als rechters of vergelijkbare juridische ervaring hebben) en vier andere leden die worden voorgedragen door de fracties in het parlement. De president en de vicepresident moeten vaste rechters zijn of zijn geweest, of vergelijkbare juridische verdiensten hebben.[208] Volgens de Zweedse regering zijn de besluiten van dit nieuwe orgaan juridisch bindend. Aangezien het nieuwe besluitvormingsorgaan binnen Siun is opgericht, heeft ook dit orgaan toegang tot relevante documenten die nodig zijn voor de taakuitoefening.

Het secretariaat van dit nieuwe besluitvormingsorgaan assisteert bij administratieve en managementtaken. Ambtenaren die werkzaam zijn bij het secretariaat zijn niet bevoegd om besluiten te nemen over de aangelegenheden van het besluitvormingsorgaan of over de toezichthoudende activiteiten van de commissieleden die Siun leiden. De werkzaamheden binnen het secretariaat worden zodanig georganiseerd dat mogelijke belangenconflicten worden vermeden.[209] De wijzigingen betreffende de instelling van dit nieuwe besluitvormingsorgaan binnen Siun zijn op 1 januari 2025 in werking getreden.[210]

### 4.3.4 IMY

*Integritetsskyddsmyndigheten* (IMY) is de algemene toezichthoudende autoriteit voor de gegevensverwerkingen van FRA en de Zweedse strijdkrachten. Zoals in paragraaf 4.2.2 is uitgelegd zijn de bevoegdheden van IMY beperkter ten opzichte van het specifieke toezicht door Siun. IMY's toezicht is namelijk in essentie beperkt tot gevallen op eigen initiatief en het houdt toezicht op veel andere instanties dan de FRA.[211] Siun's beoordeling van de verwerking van persoonsgegevens door de FRA fungeert als 'aanvulling' op het toezicht van de autoriteit voor gegevensbescherming.[212]

IMY heeft ten behoeve van haar toezicht recht op toegang tot de persoonsgegevens die worden verwerkt, informatie over en documentatie van de verwerking van persoonsgegevens, evenals toegang tot beveiligings- en beschermingsmaatregelen en bedrijfsruimten die verband houden met de verwerking van persoonsgegevens.[213] IMY heeft ook de bevoegdheid gegevensverwerking te staken als de autoriteit onrechtmatigheden vaststelt.[214]

IMY houdt ook toezicht op de gegevensverwerking door SÄPO. Tegen besluiten van de veiligheidsdienst over het corrigeren, aanvullen, wissen of beperken van persoonsgegevens op verzoek van een persoon, kan beroep worden ingesteld bij een bestuursrechter. Hetzelfde geldt

[207] SOU 2023, 87.
[208] SOU 2023, p. 21 en p. 87.
[209] Zie Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024 met verwijzing naar p. 38 van Wetsvoorstel 2023/24:136.
[210] Communicatie van Zweden naar aanleiding van de zaak Centrum för rättvisa van 25 november 2024.
[211] SOU 2025, p. 709.
[212] SOU 2023, p. 49.
[213] SOU 2023, p. 49. De commissie verwijst daarbij naar artikel 3 van de FRA-PuL wet van 2021.
[214] SOU 2023, p. 49.

voor besluiten om geen informatie te verstrekken over de verwerking van persoonsgegevens (registeruittreksels) of om voor dergelijke informatie een vergoeding te vragen.

### 4.3.3 Sin

De *Säkerhets- och integritetsskyddsnämnden* (hierna: Sin) is de autoriteit die belast is met het toezicht op het gebruik van bepaalde bijzondere bevoegdheden door rechtshandhavingsorganisaties, inclusief de binnenlandse veiligheidsdienst SÄPO. In beginsel heeft het toezicht van Sin geen betrekking op de activiteiten van de inlichtingendiensten op defensiegebied; in dat domein houdt Siun toezicht.[215]

Sin voert controles uit op verzoek van een persoon bij vermeende onrechtmatigheden bij het opleggen van bijzondere bevoegdheden en de uitoefening van dwangmaatregelen. Het voert rechtmatigheidsonderzoeken uit door middel van inspecties bij de veiligheidsdienst ter plaatse en door middel van dossieronderzoek. Sin kan op eigen initiatief inspecties uitvoeren en erop toe toezien dat politie en SÄPO geen gebruik maken van informatie die door FRA is verzameld om misdrijven te onderzoeken.[216]

SIN telt hoogstens tien commissieleden, die door de regering worden benoemd voor een vaste termijn van maximaal vier jaar. De voorzitter en vicevoorzitter zijn gewone rechters of hebben een gelijkwaardige juridische achtergrond, terwijl maximaal acht andere leden worden benoemd op voordracht van de parlementaire fracties.[217]

De Zweedse regering stuurde in 2025 een wetsvoorstel naar het parlement om de wet beter aan te laten sluiten bij de praktijk en SÄPO ruimere bevoegdheden te geven voor de verwerking van gegevens voor inlichtingendoeleinden. Tegelijkertijd wordt voorgesteld het toezicht op de gegevensverwerking aan te scherpen, met een grotere rol voor Sin bij aanvragen voor de toepassing van een selectiemechanisme en de gegevensverwerking uit bulkdatasets, waarbij Sin in bepaalde gevallen bindende bevoegdheden zou krijgen voor correctie of vernietiging van onrechtmatig verwerkte gegevens.[218] Het plan is deze nieuwe wetgeving per 1 januari 2027 in te laten gaan, met een overgangsperiode tot en met 31 december 2029.[219] Belanghebbenden moeten hun reacties op de consultatie van deze wet uiterlijk op 25 augustus 2025 indienen.[220]

Indien deze wetgeving wordt aangenomen, zouden zowel IMY als Sin parallel toezicht houden op de gegevensverwerkingsactiviteiten van SÄPO, met een extra rol voor Sin ten aanzien van aanvragen over de toepassing van een selectiemechanisme uit bulkdatasets en in procedures bij het Defensie Inlichtingenhof als voorziene beroepsinstantie.

### 4.3.5 Overige toezichthouders

In deze paragraaf worden de overige instanties genoemd die Zweedse inlichtingen- en veiligheidsdiensten controleren. De nadruk ligt in dit rapport op het rechtmatigheidstoezicht. Deze instanties worden om deze reden slechts kort omschreven.

---

[215] SOU 2023, p. 85-86.
[216] SOU 2023, p. 86.
[217] SOU 2025, p. 177.
[218] SOU 2025, p. 670.
[219] SOU 2025, p. 43-45.
[220] Zie Remiss av betänkandet Säkerhetspolisens behandling av personuppgifter (SOU 2025:49) - Regeringen.se (laatst geraadpleegd op 19 juli 2025).

*Nationale rekenkamer*

De Zweedse 'nationale auditdienst' heeft de taak om alle autoriteiten te controleren, inclusief de Zweedse inlichtingen- en veiligheidsdiensten. Deze instantie kijkt niet primair naar operationele methoden of individuele klachten, maar met name naar hoe effectief en efficiënt de diensten hun middelen gebruiken en hun wettelijke verplichtingen nakomen vanuit een auditperspectief.[221]

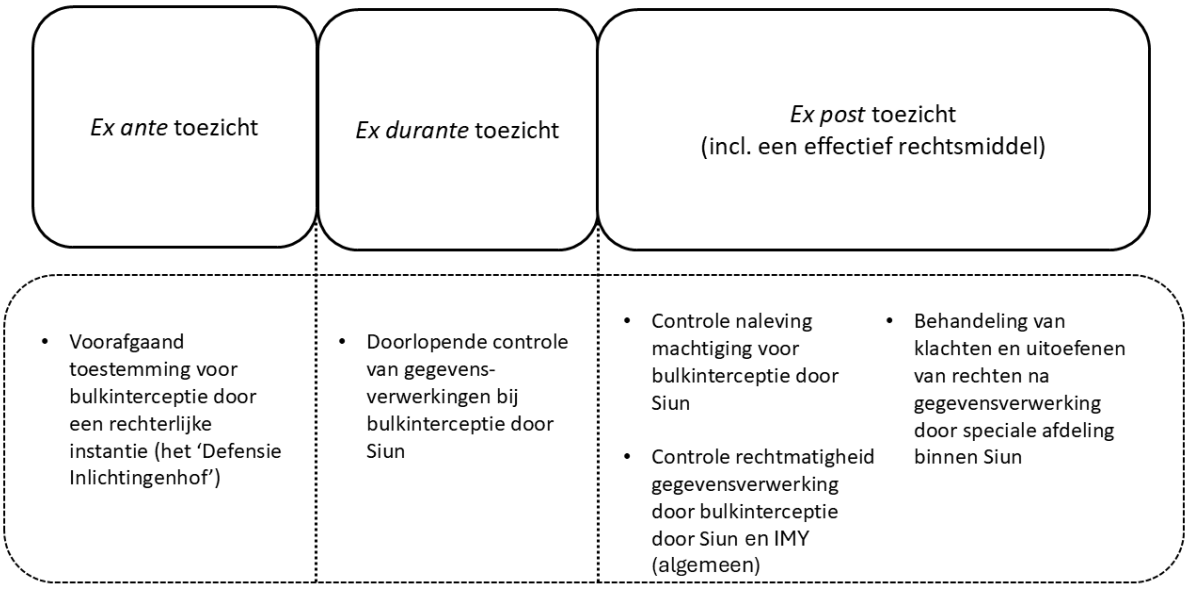
*Parlementair toezicht*

Het Ministerie van Defensie dient jaarlijks een rapport in bij het Zweedse parlement over het toezicht op defensie-inlichtingen. Dit rapport wordt eerst besproken in de Defensiecommissie en vervolgens in een plenaire vergadering. Er is geen speciale inlichtingencommissie in het Zweedse parlement.[222]

## 4.4 Conclusie

Het toezichtstelsel op de Zweedse inlichtingen- en veiligheidsdiensten onderscheidt zich van dat van veel andere landen door het functioneren van verschillende toezichthouders naast elkaar, in plaats van één gespecialiseerde instantie.

Het stelsel van toezicht ten aanzien van bulkinterceptie in het Zweden is weergegeven in Figuur 3.




Figuur 3: Het stelsel van toezicht ten aanzien van bulkinterceptie in Zweden

Het Zweedse Defensie Inlichtingenhof voert vooraf een toets uit op de rechtmatigheid voor de machtigingen voor bulkinterceptie. Vervolgens volgt gespecialiseerd toezicht (zowel ex durante als ex post) door Siun. Recent is een nieuwe afdeling binnen Siun gevestigd voor de behandeling van klachten in de ex post toezichtfase.

[221] Hansén 2023, p. 9-10.
[222] Hansén 2023, p. 9.

De beoordeling van Siun over de verwerking van persoonsgegevens door de FRA wordt gezien als aanvullend op het algemene toezicht van de Zweedse Autoriteit Persoonsgegevens (IMY). Sin geen toezicht houdt op de FRA en daarmee niet op de rechtmatigheid van de dataverzameling uit bulkinterceptie (die taak berust bij Siun). Sin wel verantwoordelijk voor het rechtmatigheidstoezicht op de binnenlandse veiligheidsdienst SÄPO.

Het is opmerkelijk dat er geen specifieke regeling bestaat voor de verwerking van gegevens door het Zweedse nationaal cybersecuritycentrum, een samenwerkingsverband van diverse instanties (waaronder FRA en SÄPO), ondanks dat dit centrum verantwoordelijk is voor het aanpakken, opsporen en voorkomen van IT-incidenten die de veiligheid van Zweden in gevaar kunnen brengen.

De Zweedse regering is voornemens het mandaat van FRA voor bulkinterceptie en de verwerking van bulkgegevens door SÄPO uit te breiden, waarbij gelijktijdig het toezicht wordt aangescherpt. Deze wet is tot en met 25 augustus 2025 in consultatie. De belangrijkste wijzigingen betreffen een uitbreiding van de taken van het Defensie Inlichtingenhof en een versterking van de rol van Sin. Het Defensie Inlichtingenhof zou in de toekomst als beroepsinstantie kunnen fungeren bij bindende besluiten over gegevensverwerking, terwijl Sin een grotere rol zal spelen bij aanvragen voor het toepassen van selectiemechanismen en de verwerking van bulkdatasets, met mogelijk bindende bevoegdheden om onrechtmatig verwerkte gegevens te corrigeren of te vernietigen. Bij aanname van deze wetgeving zullen zowel IMY als Sin parallel toezicht houden op de gegevensverwerkingsactiviteiten van SÄPO.

# Hoofdstuk 5: Het toezichtstelsel in Frankrijk

Dit hoofdstuk beschrijft het toezichtstelsel op de Franse inlichtingen- en veiligheidsdiensten. Eerst wordt een overzicht gegeven van deze diensten, inclusief hun specifieke taken (zie paragraaf 5.1). De wet- en regelgeving en het toezicht op bulkinterceptie worden beschreven in paragraaf 5.2. Vervolgens biedt paragraaf 5.3 een overzicht van algemene toezichtstelsel van toezicht op de inlichtingen- en veiligheidsdiensten van Frankrijk. Paragraaf 5.4 biedt een samenvatting met de belangrijkste kenmerken en werking van het Franse toezichtstelsel.

## 5.1 De inlichtingen- en veiligheidsdiensten van Frankrijk

Frankrijk kent bijna twintig inlichtingen- en veiligheidsdiensten. Het Franse wetboek inzake binnenlandse veiligheid bepaalt welke diensten bevoegd zijn om de in de wet omschreven inlichtingentechnieken te gebruiken.

De zes gespecialiseerde inlichtingendiensten, aangeduid als de “eerste cirkel”, hebben het recht om de meeste bij wet vastgestelde inlichtingenmethoden toe te passen.[223] De overige diensten, die bekend staan als de diensten van de “tweede cirkel”, hebben slechts beperkte toegang tot deze technieken.[224] De zes gespecialiseerde inlichtingendiensten uit de eerste cirkel zijn door de Franse wetgever belast met het verzamelen, analyseren en verstrekken aan de regering van inlichtingen over geopolitieke en strategische kwesties, evenals bedreigingen en risico’s die het voorbestaan van Frankrijk kunnen beïnvloeden. De wet specificeert dat zij moeten bijdragen aan de verzameling van inlichtingen over deze kwesties en daarop anticiperen, en dergelijke risico's en bedreigingen moeten voorkomen en tegengaan.[225]

De opsomming van inlichtingen- en veiligheidsdiensten is in deze paragraaf beperkt tot de eerste cirkel van zes inlichtingen- en veiligheidsdiensten, plus het nationale cybersecuritycentrum van Frankrijk.[226]

### 5.1.1 DGSE

De *Direction générale de la sécurité extérieure* (DGSE) is verantwoordelijk voor het verzamelen en benutten van inlichtingen die relevant zijn voor de veiligheid van Frankrijk, en voor het opsporen en tegenhouden van spionageactiviteiten buiten het nationale grondgebied, gericht tegen Franse belangen.

De organisatie staat onder het gezag van een directeur-generaal die rechtstreeks rapporteert aan de minister van Defensie. Het directoraat-generaal Buitenlandse Veiligheid is opgericht bij een decreet van 2 april 1982.[227]

[223] Zie artikel L811-2 *Code de la sécurité intérieure* (het Wetboek op de binnenlandse veiligheid).
[224] De inlichtingen- en veiligheidsdiensten van de tweede cirkel zijn ondergebracht bij het Directoraat-Generaal van de Nationale Politie, het Directoraat-Generaal van de Nationale Gendarmerie, en de *Direction de l'Administration Pénitentiaire* (Directie Penitentiaire Inrichtingen). Zie Notre rôle | CNCTR (laatst geraadpleegd op 18 juli 2025).
[225] Article L811-2 Code de la sécurité intérieure.
[226] De eerste zes diensten zijn aangewezen bij een besluit dat wordt genomen door Conseil D’Etat (de Franse Raad van State). De lijst is opgenomen in artikel R. 811-1 van de Code de la sécurité intérieure.
[227] Les principaux services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).

### 5.1.2 DGSI

De *Direction générale de la sécurité intérieure* (DGSI) is verantwoordelijk voor het opsporen, centraliseren en analyseren van inlichtingen met betrekking tot de nationale veiligheid of de fundamentele belangen van Frankrijk. Het is een afdeling van de Franse nationale politie en valt onder de verantwoordelijkheid van het Ministerie van Binnenlandse Zaken. Het directoraat-generaal Binnenlandse Veiligheid is opgericht bij een decreet van 30 april 2014, waarin de taken en organisatie van het directoraat-generaal zijn vastgelegd.

De dienst is verantwoordelijk voor het voorkomen van en assisteren bij elke vorm van buitenlandse inmenging, terroristische misdrijven of misdrijven die de staatsveiligheid, territoriale integriteit of het voortbestaan van de instellingen van de republiek Frankrijk ondermijnen. Daarnaast draagt het bij aan de preventie en bestrijding van activiteiten die de nationale defensiegeheimen of het economische, industriële of wetenschappelijke potentieel van het land ondermijnen, evenals activiteiten die verband houden met de verwerving of vervaardiging van massavernietigingswapens.

Tot slot draagt de DGSI bij aan de handhaving en opsporing van activiteiten van internationale criminele organisaties die de nationale veiligheid kunnen aantasten, en aan het voorkomen en bestrijden van cybercriminaliteit.[228]

### 5.1.3 DNRED

De *Direction nationale du renseignement et des enquêtes douanières* (DNRED) is verantwoordelijk voor de uitvoering van het inlichtingen-, controle- en fraudebestrijdingsbeleid van het directoraat-generaal Douane en Accijnzen. DNRED rapporteert aan de ministeries van Economie en Financiën. Het werd opgericht bij een decreet van 1 maart 1988. [229]

### 5.1.4 DRM

De *Direction du renseignement militaire* (DRM) is de inlichtingendienst van de Franse strijdkrachten en rapporteert aan de chef-staf van de strijdkrachten. Het voorziet in de behoefte aan militaire inlichtingen, met name voor het uitvoeren van operaties. De Directie Militaire Inlichtingen is opgericht bij decreet van 16 juni 1992.[230]

### 5.1.5 DRSD

De *Direction du renseignement et de la sécurité de la défense* (DRSD) is een inlichtingendienst met als taak de beveiliging van personeel, informatie, apparatuur en gevoelige installaties voor het ministerie van Defensie. De dienst heeft ook contra-inlichtingentaak uit om elke dreiging in de vorm van terrorisme, spionage, subversie, sabotage of georganiseerde misdaad tegen te gaan. De dienst werd opgericht in 1981.[231]

[228] Les principaux services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[229] Les principaux services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[230] De taken van deze directie zijn omschreven in de artikelen D.3126-10 en D.3126-14 van het Wetboek van Defensie en de organisatie ervan is vastgelegd in het decreet van 30 maart 2016.
[231] Les principaux services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).

### 5.1.6 Tracfin

De *Traitement du renseignement et action contre les circuits financiers clandestins* (Tracfin) is verantwoordelijk voor inlichtingen met betrekking tot criminele financiële circuits, witwassen, en de financiering van terrorisme. De dienst staat onder leiding van de minister van Economie en Financiën. Tracfin werd opgericht bij een decreet van 9 mei 1990.[232]

### 5.1.7 ANSSI

De *Agence nationale de la sécurité des systèmes d'information* (ANSSI) is het Franse nationaal cybersecuritycentrum. Hoewel het volgens de Franse wet geen inlichtingen- en veiligheidsdienst is, verdient het toch vermelding.

ANSSI is verantwoordelijk voor het beschermen van overheidsnetwerken en kritieke infrastructuren tegen cyberaanvallen, het toezicht houden op de beveiliging van informatie- en communicatiesystemen binnen de publieke sector, het coördineren van de respons op cyberincidenten via het nationale *Computer Emergency Response Team* (CERT-FR), en het uitvaardigen van richtlijnen en normen voor cyberbeveiliging in Frankrijk. ANSSI valt onder het *Secrétariat général de la défense et de la sécurité nationale*, dat direct onder het kabinet van de Franse premier ressorteert.[233]

Uit een evaluatie van 3 oktober 2023 blijkt dat ANSSI een uitbreiding van haar verantwoordelijkheden heeft gekregen op het gebied van detectie van cyberaanvallen.[234] Op basis van de '*Loi de Programmation Militaire* 2019-2025' van 2018, mogen telecomproviders in Frankrijk dreigingsdetectie uitvoeren op het netwerk van hun klanten met sensoren die geschikt zijn voor de technische handtekeningen voor detectie van cyberaanvallen door ANSSI.[235] Bovendien is ANSSI bevoegd om, in geval van een 'ernstige en bewezen dreiging', tijdelijk een lokaal detectiesysteem te implementeren op de informatiesystemen van een Franse host.[236] Dit geldt wanneer de aanval gericht is op de informatiesystemen van beheerders van vitale en kritieke infrastructuren of overheidsinstellingen.[237]

## 5.2 De uitoefening van bulkinterceptie in Frankrijk

Deze paragraaf beschrijft de ontwikkeling van het juridisch kader voor bulkinterceptie in Frankrijk, gevolgd door een bespreking van het ex ante toestemmingsproces en een overzicht van de beroepsprocedures op bindende beslissingen door de Franse toezichthouders. Tot slot wordt het ex post toezicht ten aanzien van bulkinterceptie beschreven.

---

[232] Les principaux services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[233] Missions | ANSSI (laatst geraadpleegd op 18 juli 2025).
[234] Zie het rapport 'Strategische evaluatie van cyberdefensie' van 3 oktober 2023 (laatst geraadpleegd op 18 juli 2025).
[235] LOI DE PROGRAMMATION MILITAIRE 2019/2025 : une protection accrue contre les attaques informatiques - DS-Avocats-global. Zie ook Martin Untersinger, 'Cybersécurité : le gouvernement veut mettre les télécoms à contribution pour détecter les attaques', *lemonde.fr*, 8 februari 2018 (laatst geraadpleegd op 18 juli 2025).
[236] In het rapport 'Strategische evaluatie van cyberdefensie' van 3 oktober 2023 wordt verwezen naar een wettelijke grondslag in artikel L2321-2-1 *Code de la Défense*.
[237] De bevoegdheid van ANSSI om tijdelijk detectieapparatuur te installeren bij Franse hostingproviders in geval van ernstige dreiging werd eerder beschreven op de officiële website van ANSSI (pagina "Renforcement de la détection des cyberattaques", ssi.gouv.fr), maar deze pagina is inmiddels niet meer beschikbaar.

### 5.2.1 Ontwikkeling juridisch kader voor bulkinterceptie

Na een veroordeling van Frankrijk door het EHRM in de zaken *Huvig*[238] en *Kruslin*[239] tegen Frankrijk, stelde de regering na 1990 wetgeving op voor interceptie door inlichtingen- en veiligheidsdiensten. Dit resulteerde in een wet van 10 juli 1991 die de bevoegdheid tot het onderscheppen van telecommunicatie regelde, evenals de controle daarop door een onafhankelijke autoriteit. De *Commission nationale de contrôle des interceptions de sécurité* was aanvankelijk alleen bevoegd tot het controleren van onderschepte communicatie.[240]

Gedurende bijna 25 jaar ontbrak externe controle voor een groot deel van de inlichtingentechnieken die door Franse diensten werden gebruikt, totdat de *Code de la sécurité intérieure* van 3 oktober 2015 werd aangenomen. Deze wet legde de voorwaarden vast voor het toepassen van alle inlichtingentechnieken die de Franse inlichtingendiensten mogen gebruiken en introduceerde een nieuwe toezichthouder: de *Commission nationale de contrôle des techniques de renseignement* (CNCTR). De CNCTR verving de oude toezichthouder en is (nog steeds) verantwoordelijk voor het toezicht op de naleving van het nieuwe wettelijke kader.[241]

De Franse wet bevat een uitputtende lijst van bijzondere bevoegdheden ("inlichtingentechnieken" genoemd) voor de inlichtingen- en veiligheidsdiensten en bepaalt de voorwaarden voor hun gebruik, zoals vastgelegd in titel V en VIII van de Code de la sécurité intérieure.[242] Zoals in paragraaf 5.1 is uitgelegd mag niet elke dienst alle bijzondere bevoegdheden inzetten.

Met betrekking tot bulkinterceptie bestaat er gedetailleerde wet- en regelgeving die verwijst naar het 'onderscheppen en exploiteren van internationale elektronische communicatie'.[243] Alleen de zes genoemde inlichtingendiensten uit de eerste cirkel hebben de bevoegdheid om internationale elektronische communicatie te onderscheppen en te gebruiken. Deze bevoegdheid moet gericht zijn op het verzamelen van inlichtingen over personen of entiteiten die zich in het buitenland bevinden, tenzij de wet een uitzondering voorziet. Het middel mag worden ingezet ter bescherming van de volgende doeleinden:

1. De territoriale integriteit en nationale defensie;
2. 'Grote belangen van het buitenlands beleid', het nakomen van de Europese en internationale verplichtingen van Frankrijk en het voorkomen van elke vorm buitenlandse inmenging;
3. Grote economische, industriële en wetenschappelijke belangen van Frankrijk;
4. Het voorkomen van terrorisme;
5. Het voorkomen van: a) aanvallen op de Franse republikeinse staatsvorm; b) acties gericht op het in stand houden of opnieuw samenstellen van groepen die ontbonden zijn

[238] EHRM 24 april 1990, nr. 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584 (*Huvig t. Frankrijk*).
[239] EHRM 24 april 1990, nr. 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin t. Frankrijk*).
[240] Zie L'instauration progressive d'un contrôle de l'activité des services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[241] Idem.
[242] Zie Les techniques de renseignement contrôlées par la CNCTR | CNCTR (laatst geraadpleegd op 18 juli 2025).
[243] Wet n° 2015-1556 van 30 november 2015 'relative aux mesures de surveillance des communications électroniques internationales'.

krachtens wetgeving; en c) collectief geweld dat ernstige schade kan toebrengen aan de openbare orde;
6. Het voorkomen van georganiseerde misdaad en delinquentie;
7. Het voorkomen van de verspreiding van massavernietigingswapens.[244]

De wet vereist dat inlichtingendiensten elk verzoek om toestemming voldoende gedetailleerd motiveren. De eerdergenoemde organisatie 'GIC' is onder andere verantwoordelijk voor het centraliseren van alle verzoeken tot het gebruik van inlichtingentechnieken het beheert de technische infrastructuur waarmee bijvoorbeeld intercepties of geautomatiseerde gegevensverwerkingen worden uitgevoerd. Het stuurt bovendien de resultaten van het gebruik van de inlichtingenmiddelen door naar de bevoegde inlichtingendiensten. Dit proces en deze organisatie is opgezet om ongeoorloofde toegang tot gegevens te voorkomen en om juridische controle mogelijk te maken.[245]

### 5.2.2 Ex ante toestemming

Het proces voor de inzet van bulkinterceptie als inlichtingenmethode in Frankrijk kent de volgende structuur.[246]

Voorafgaand aan de inzet zijn twee afzonderlijke machtigingen vereist: één voor interceptie en één voor exploitatie.[247] De Franse premier moet door middel van een gemotiveerd besluit toestemming geven voor interceptie. Voor de exploitatie van de gegevens is een aanvullende toestemming van de premier vereist, die wordt verleend na overleg en advies van de CNCTR.[248] De Franse wet schrijft voor dat inlichtingendiensten elk verzoek om toestemming met voldoende detail moeten motiveren. Dit omvat het specificeren van de techniek waarvoor toestemming wordt aangevraagd, de beoogde doeleinden, de rechtvaardiging voor het gebruik van deze bevoegdheid, de identiteit van het doelwit en, indien van toepassing, de locatie waar het apparaat voor het verzamelen van inlichtingen zal worden geïnstalleerd.[249]

Beide machtigingen zijn maximaal vier maanden geldig. Ze kunnen betrekking hebben op een individu, een groep personen, een "organisatie" (van welke aard dan ook) of een specifiek geografisch gebied.[250] De interceptie mag niet gericht zijn op communicatie van personen die zich op Frans grondgebied bevinden. Dit betekent dat het niet gericht mag zijn op personen met abonneenummergegevens die tot het nationale grondgebied kunnen worden herleid, zoals telefoonnummers beginnend met het netnummer +33.[251]

Na indiening van een verzoek om toepassing van een inlichtingenmiddel bij de CNCTR, geeft de commissie een gunstig of ongunstig advies over de inzet aan de Franse premier. Zodra een

[244] Zie artikel L811-1 en 811-3 (Wet nr. 2015-912 van 24 juli 2015) en Les finalités pouvant légalement justifier le recours à des techniques de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[245] Zie Les techniques de renseignement contrôlées par la CNCTR | CNCTR en Le contrôle de la mise en œuvre des techniques de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[246] Deze procedure is omschreven in artikel L821-1 van de Binnenlandse Veiligheidswet (gewijzigd bij LOI n°2021-998 van 30 juli 2021 - art. 18).
[247] Artikel 854-2 Code de la sécurité intérieure.
[248] Dit wordt in Nederland de 'selectiebevoegdheid' genoemd.
[249] Zie Les finalités pouvant légalement justifier le recours à des techniques de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[250] Zie ook artikel L854-1 Code de la sécurité intérieure.
[251] Zie Zie Les techniques de renseignement contrôlées par la CNCTR | CNCTR (laatst geraadpleegd op 18 juli 2025).

aanvraag bij de CNCTR is ingediend, heeft de toezichthouder 24 uur de tijd om tot een besluit te komen. De commissie controleert tijdens dit proces of de juiste procedure is gevolgd, of de verstrekte redenen voldoende zijn en verifieert (a) de gerechtvaardigde doelen, (b) de motivatie van het object van onderzoek, (c) de proportionaliteit van de maatregel, en (d) voldaan is aan het subsidiariteitsvereiste.[252] De CNCTR beperkt zich niet tot het geven van gunstige of ongunstige adviezen. Zij motiveert elk ongunstig advies en legt de betrokken diensten uit waarom zij tot een dergelijk advies is gekomen, zodat deze kennis kan worden gebruikt bij toekomstige verzoeken.

### 5.2.3 Beroepsprocedure

Als de premier toestemming geeft ondanks een ongunstig advies van de CNCTR, moet de commissie de zaak onmiddellijk voorleggen aan de Conseil d'État, met het verzoek aan de administratieve rechter om de wettigheid van de beslissing te toetsen en eventueel nietig te verklaren. Dit beroep wordt ingesteld bij een gespecialiseerde kamer van de Conseil d'État. De leden van deze kamer zijn ambtshalve gemachtigd om staatsgeheime stukken te behandelen en doen binnen 24 uur uitspraak, in eerste aanleg en laatste aanleg zonder verdere beroepsmogelijkheden.

Het besluit van de premier mag niet worden uitgevoerd vóór het verstrijken van deze termijn, tenzij in specifieke, gemotiveerde gevallen waarin de premier expliciet onmiddellijke uitvoering beveelt.[253]

### 5.2.4 Ex post toezicht

De CNCTR kan controles uitvoeren vanaf het begin tot het einde van een operatie.[254] De CNCTR houdt bijvoorbeeld toezicht op de bewaartermijnen van gegevens die met behulp van een techniek zijn verzameld en die geen directe inlichtingenwaarde hebben. De commissie zorgt ervoor dat de inlichtingendiensten deze gegevens binnen de vastgestelde termijnen vernietigen, afhankelijk van het type informatie (vier jaar voor verbindingsgegevens en slechts 30 dagen voor woorden of beelden).[255]

De CNCTR oefent ook ex post toezicht uit naar aanleiding van een klacht van een belanghebbende. Na ontvangst van een klacht beoordeelt de CNCTR of een inlichtingstechniek op rechtmatige wijze is ingezet. De (stafmedewerkers van de) CNCTR voert deze controle uit. Indien een onrechtmatigheid wordt vastgesteld, zal zij de dienst gelasten de lopende inlichtingentechniek stop te zetten en alle verzamelde gegevens te vernietigen. In geval van weigering kan de Commissie de zaak voorleggen aan de premier of, indien nodig, zelf beroep aantekenen bij de Conseil d'État (zie ook paragraaf 2.1.3).[256]

Het bovenstaande betekent de CNCTR de centrale toezichthoudende instantie is op de inlichtingen- en veiligheidsdiensten van Frankrijk. Het heeft zowel een taak vooraf op de inzet van bulkinterceptie, tijdens de uitvoering en houdt toezicht achteraf. Daarbij behandelt het ook

[252] Zie Le contrôle préalable à la mise en œuvre de techniques de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[253] Zie FAQ | CNCTR (laatst geraadpleegd op 18 juli 2025).
[254] Zie Le contrôle de la mise en œuvre des techniques de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[255] Idem.
[256] Artikel L. 833-8 Code de la sécurité intérieure.

nog als eerste instantie de klachten van verzoekers over vermeend onrechtmatig handelen van de Franse inlichtingen- en veiligheidsdiensten.

## 5.3 Het stelsel van toezicht

Deze paragraaf beschrijft het Franse toezichtstelsel op de inlichtingen- en veiligheidsdiensten. Ook worden de 'overige toezichthouders' kort beschreven, zoals de parlementaire toezichthouders en de nationale Rekenkamer.

### 5.3.1 CNCTR

De *Commission nationale de contrôle des techniques de renseignement* (CNCTR) werd in 2015 opgericht als toezichthouder op de Franse inlichtingen- en veiligheidsdiensten (zie ook paragraaf 5.2.1).[257] De CNCTR voert sindsdien de rechtmatigheidsonderzoeken uit met betrekking tot het gebruik van de inlichtingenmiddelen door de Franse inlichtingen- en Veiligheidsdiensten.[258]

De CNCTR kan worden getypeerd als een 'onafhankelijke administratieve autoriteit'. De autoriteit is onafhankelijk van het parlement en de regering, en vindt haar achtergrond in de het beginsel van de scheiding der machten en de vereisten voor staatsgeheime informatie met betrekking tot de activiteiten van de inlichtingendiensten.[259] De voorzitter van de CNCTR wordt door de president van Frankrijk gekozen uit leden van de Conseil d'État of het hooggerechtshof (*Cour de cassation*). De autoriteit bestaat uit negen commissieleden: vier leden van het parlement en de senaat, twee leden van de Conseil d'État, twee leden van de Cour de cassation, en één deskundige op het gebied van elektronische communicatie. De ambtstermijn van de leden is zes jaar en herbenoeming is niet mogelijk.[260] Een statuut waarborgt hun onafhankelijkheid ten opzichte van de commissie. Zij mogen bijvoorbeeld geen instructies ontvangen over de uitoefening van hun werkzaamheden. Wetgeving verbiedt bovendien een direct of indirect belang bij de inlichtingendiensten of bij operatoren van elektronische communicatie en internetproviders. De commissieleden worden ondersteund door een secretariaat.[261]

Eind 2024 beschikte de CNCTR over een team van 22 medewerkers, onder leiding van een secretaris-generaal. Het team bestond uit onder meer 14 projectfunctionarissen en vier ondersteunende medewerkers, en één systeembeheerder.[262] De belangrijkste taak van de ambtenaren is het onderzoeken van verzoeken voor het gebruik van inlichtingenmiddelen en het uitvoeren van *ex post* toezicht, onder toezicht van een lid van de commissie.[263]

De CNCTR voert rechtmatigheidscontroles uit in alle fasen van het gebruik van inlichtingentechnieken, te weten de verzameling, verdere verwerking en verstrekking van gegevens. De huidige Franse wetgeving sluit uit dat de CNCTR toezicht houdt op inlichtingen die zijn verkregen door de uitwisseling van gegevens met inlichtingen- en veiligheidsdiensten

[257] L'instauration progressive d'un contrôle de l'activité des services de renseignement | CNCTR (laatst geraadpleegd op 18 juli 2025).
[258] Artikel L. 833-1 Code de la sécurité intérieure.
[259] Antwoord op schriftelijke vragen aan de CNCTR van 23 april 2024.
[260] Artikel L. 831-1 Code de la sécurité intérieure.
[261] Zie CNCTR | La Commission Nationale de Contrôle des Techniques de Renseignement (laatst geraadpleegd op 18 juli 2025).
[262] Jaarverslag CNCTR 2024, p. 190.
[263] Jaarverslag CNCTR 2024, p. 191.

buiten Frankrijk.[264] In haar jaarverslagen pleit de toezichthouder voor wijzigingen en een passend juridisch kader voor dergelijke internationale uitwisselingen, gezien de mogelijke gevolgen voor de persoonlijke levenssfeer van Franse burgers of personen die in Frankrijk verblijven.[265]

In 2024 voerde de CNCTR 123 inspecties uit. Deze controles worden uitgevoerd door middel van (1) bezoeken aan de gebouwen van de inlichtingendiensten, waar documenten worden gecontroleerd en controles ter plaatse worden uitgevoerd in direct contact met betrokken ambtenaren, en (2) op afstand, vanuit haar eigen gebouwen, met behulp van beveiligde IT-instrumenten die beschikbaar zijn gesteld door zowel de CNCTR, als de inlichtingendiensten, of het GIC. Naar eigen zeggen voert de CNCTR dagelijks online controles uit, welke ook worden gebruikt ter voorbereiding van dossiercontroles en voor controles ter plaatse in de gebouwen van de diensten.[266]

De resultaten van de onderzoeksactiviteiten van de CNCTR worden voornamelijk gepubliceerd via een uitgebreid jaarverslag. Dit verslag bevat statistische gegevens over het aantal verzoeken om het gebruik van inlichtingenmiddelen door de inlichtingendiensten, de in deze verzoeken vermelde doeleinden, het aantal ongunstige adviezen die zijn uitgebracht en het aantal personen dat met behulp van deze technieken is gevolgd.[267] Daarnaast publiceert de CNCTR haar adviezen over het wettelijk kader voor inlichtingentechnieken, zowel voor het parlement als in adviezen op eigen initiatief of op verzoek van de regering.[268]

Zoals beschreven in paragraaf 2.1.3 en 5.2.3 voert de CNCTR ook onderzoeken uit naar aanleiding van klachten. In alle gevallen wordt de betrokkene geïnformeerd over de uitgevoerde controles.[269]

Ten slotte heeft de CNCTR ook een taak met betrekking tot het behandelen van meldingen van klokkenluiders. Ambtenaren van de inlichtingendiensten die bij de uitoefening van hun functie kennis hebben van misstanden, kunnen deze feiten uitsluitend onder de aandacht van de CNCTR brengen. De commissieleden van de CNCTR kunnen naar aanleiding daarvan een onderzoek instellen.[270]

### 5.3.2 Conseil D'État

De Conseil d'État fungeert als hoogste beroepsinstantie op het gebied van bestuursrechtspraak. Zoals reeds vermeld in paragraaf 2.1.3, is de Conseil d'État bevoegd om zaken te behandelen waarin belanghebbenden bezwaar maken tegen vermeend onrechtmatig gebruik van inlichtingentechnieken. Deze rechtbank kan ook verzoeken om voorlopige maatregelen met betrekking tot de Franse inlichtingen- en veiligheidsdiensten beoordelen.

---

[264] Zie Délégation parlementaire au renseignement - rapport d'activité n° 506 2019-2020, van 11 juni 2020.
[265] Zie bijv. het CNCTR jaarverslag van 2022, p. 69 e.v.; CNCTR jaarverslag 2023, p. 80 e.v.; CNCTR jaarverslag 2024, p. 103.
[266] Jaarverslag CNCTR 2024, p. 60.
[267] In 2023 vertegenwoordigden de ongunstige adviezen van de CNCTR bijvoorbeeld 1,2% van het totaal aantal adviezen.
[268] CNCTR | La Commission Nationale de Contrôle des Techniques de Renseignement (laatst geraadpleegd op 18 juli 2025). De jaarverslagen zijn te vinden op CNCTR.fr, in zowel het Engels als in het Frans.
[269] Op grond van artikel L. 833-4 Code de la sécurité intérieure.
[270] Artikel L. 861-3 Code de la sécurité intérieure. Zie ook Comment saisir la commission ? | CNCTR (laatst geraadpleegd op 18 juli 2025).

De Conseil d'État behandeld de zaken in met een gespecialiseerde kamer. De leden van deze kamer mogen alle documenten en informatie inzien die ze nodig hebben om hun gerechtelijke taak uit te voeren, met inbegrip van staatsgeheime informatie. Ze mogen toegang vragen tot alle documenten die in het bezit zijn van de inlichtingendiensten en de CNCTR. Om staatsgeheimen te beschermen, is toegang tot dergelijke informatie echter beperkt tot de leden van deze rechtbank.

Wanneer de rechtbank vaststelt dat een techniek voor het vergaren van inlichtingen onrechtmatig is ingezet of gegevens onrechtmatig zijn verwerkt, kan zij de machtiging intrekken en de vernietiging van de onrechtmatig verkregen informatie bevelen. Zonder vertrouwelijke informatie te openbaren, stelt de rechtbank de betrokken partij of de verwijzende rechter op de hoogte van een onrechtmatige handeling. Op verzoek kan er een schadevergoeding aan de betrokken partij worden toegekend.[271]

### 5.3.3 Overige toezichthouders

Deze paragraaf beschrijft de overige instanties die de Franse inlichtingen- en veiligheidsdiensten controleren. De nadruk ligt in dit rapport op het rechtmatigheidstoezicht. Deze instanties worden om deze reden slechts kort omschreven.[272]

*De nationale Rekenkamer*

De Franse Nationale Rekenkamer, de *Cour des Comptes*, houdt toezicht op de financiële bestedingen van diverse overheidsinstanties, waaronder de inlichtingen- en veiligheidsdiensten. De Cour des Comptes voert audits uit om te controleren of middelen efficiënt en rechtmatig worden gebruikt. Haar bevindingen worden gerapporteerd aan de regering en het parlement. Deze rapporten zijn vaak openbaar toegankelijk.[273]

*Parlementair toezicht*

Sinds 9 oktober 2007 voert de ‘parlementaire delegatie inlichtingenwerk’ ook toezicht uit op de Franse inlichtingen- en veiligheidsdiensten. Dit orgaan is samengesteld uit leden van zowel de Senaat als het Parlement. De CNCTR wordt regelmatig geraadpleegd door het Parlement, met name door de deze delegatie, om haar bevindingen over de toepassing van de wet voor te leggen aan de commissieleden.

Deze delegatie kan ook aanbevelingen doen aan de regering en het parlement over beleid en wetgeving betreffende de inlichtingen- en veiligheidsdiensten. De parlementaire delegatie inlichtingenwerk publiceert jaarlijks rapporten over haar bevindingen en aanbevelingen.[274]

*Telecommunicatieautoriteit*

De *Autorité de régulation des communications électroniques et des postes* (ARCEP) houdt toezicht op de telecommunicatiesector en ook op het Franse nationaal cybersecuritycentrum ANSSI. Deze instantie overlegt eveneens met de CNCTR en kan zaken doorverwijzen naar de

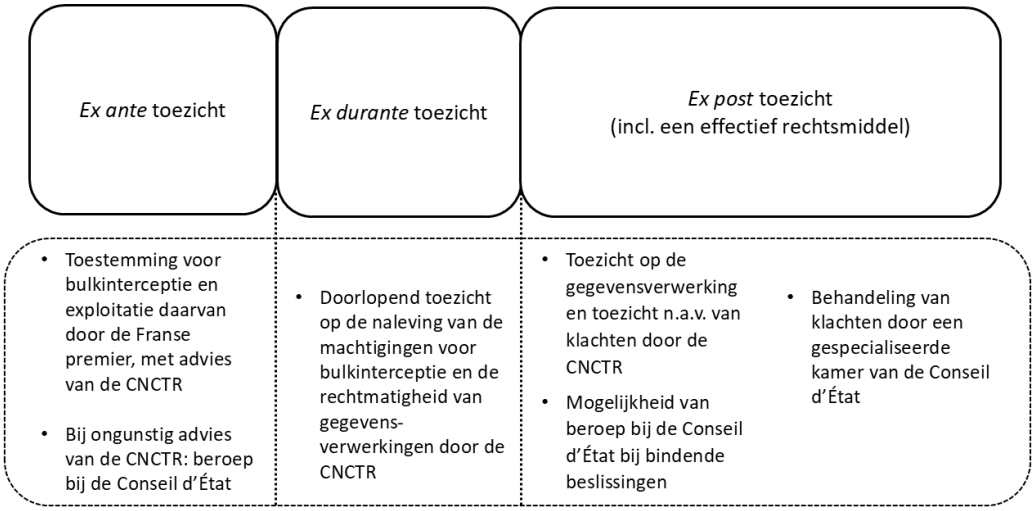
[271] Zie verder paragraaf 2.1.3.
[272] De Franse Autoriteit Persoonsgegevens lijkt bijvoorbeeld geen rol van betekenis te spelen in dit domein en wordt daarom in deze paragraaf niet genoemd.
[273] Zie Page d'accueil | Cour des comptes (laatst geraadpleegd op 18 juli 2025).
[274] Délégation parlementaire au renseignement | Sénat (laatst geraadpleegd op 18 juli 2025).

CNCTR. Tot op heden zijn er geen voorbeelden bekend van rapportages die voortvloeien uit dergelijke samenwerkingen.

## 5.4 Conclusie

Frankrijk beschikt over een complex stelsel van inlichtingen- en veiligheidsdiensten, bestaande uit bijna twintig diensten, waarvan zes inlichtingen- en veiligheidsdiensten onder bepaalde voorwaarden bevoegd zijn tot bulkinterceptie. De wettelijke kaders die het functioneren van deze diensten en hun toezichthouders regelen, zijn sinds 2015 van toepassing.

De beslissing van 10 december 2024 van het EHRM in de zaak *Contrafraternelle de la Presse e.a.* bevestigt dat Frankrijk beschikt over een voldoende solide toezichtstelsel met effectieve rechtsmiddelen voor betrokkenen. Het stelsel van toezicht ten aanzien van bulkinterceptie in Frankrijk is weergegeven in Figuur 4.




Figuur 4: Het stelsel van toezicht ten aanzien van bulkinterceptie in Frankrijk

De CNCTR fungeert als een onafhankelijke, gespecialiseerde toezichthouder en houdt toezicht op alle fasen van bulkinterceptie en andere gegevensverwerkingen. Deze instantie kan bindende beslissingen nemen. Opvallend is dat in Frankrijk het toezicht van de CNCTR op de uitwisseling van gegevens met buitenlandse inlichtingen- en veiligheidsdiensten is uitgesloten.

Kenmerkend aan het Franse stelsel is de grote rol die voor het toezicht is toebedeeld aan de rechterlijke macht via de Conseil d'État. Een bijzondere kamer binnen de Conseil d'État fungeert als beroepsinstantie bij klachten en bij bepaalde beslissingen van de CNCTR.

Tot slot is opmerkelijk dat het Franse nationale cybersecuritycentrum (ANSSI) onder toezicht valt van een telecomtoezichthouder, terwijl het is ondergebracht bij het Ministerie van Defensie en over uitgebreide bevoegdheden beschikt voor de detectie van cyberaanvallen. In Denemarken is dit toezicht bijvoorbeeld belegd bij de gespecialiseerde toezichthouder op inlichtingen- en veiligheidsdiensten. Wel kan de telecomtoezichthouder overleggen met en zaken doorverwijzen naar de CNCTR.

# Hoofdstuk 6: Het toezichtstelsel in het Verenigd Koninkrijk

Dit hoofdstuk beschrijft het toezichtstelsel op de inlichtingen- en veiligheidsdiensten van het Verenigd Koninkrijk. Het biedt in paragraaf 6.1 een overzicht van deze diensten en hun taken, met inbegrip het nationaal cybersecuritycentrum. De regeling en het toezicht op bulkinterceptie als bijzondere bevoegdheid wordt beschreven in paragraaf 6.2. Paragraaf 6.3 geeft vervolgens een overzicht van het algemene toezichtstelsel op deze diensten, waarna paragraaf 6.4 een samenvatting geeft van de belangrijkste kenmerken en werking van het toezichtstelsel in het Verenigd Koninkrijk.

## 6.1 De inlichtingen- en veiligheidsdiensten van het Verenigd Koninkrijk

Het inlichtingenapparaat van het Verenigd Koninkrijk wordt beschouwd als een van de meest geavanceerde van Europa.[275] Deze diensten bestaan al sinds het begin van de twintigste eeuw, maar de formele vastlegging van hun bevoegdheden kwam pas later met de *Security Service Act 1989* en de *Intelligence Services Act 1994*.[276]

De inlichtingengemeenschap in het Verenigd Koninkrijk bestaat uit de volgende drie diensten:

1. de *Security Service* (MI5);
2. de *Secret Intelligence Service* (SIS) (ook wel MI6 genoemd); en
3. de *Government Communications Headquarters* (GCHQ).[277]

De operaties van alle drie de diensten zijn in het algemeen gericht op de bescherming van de nationale veiligheid, het voorkomen of opsporen van criminaliteit, en het beschermen van de economische belangen van het Verenigd Koninkrijk.[278] De diensten werken nauw met elkaar samen, maar hun specifieke missie, focus en taken verschillen van elkaar. Hieronder volgt een kort beschrijving van elke dienst met hun taken, plus het nationaal cybersecuritycentrum van het Verenigd Koninkrijk.

### 6.1.1 MI5

MI5 is de Britse binnenlandse veiligheidsdienst, die de Britse beschermt tegen bedreigingen van de nationale veiligheid burgers (zowel in het Verenigd Koninkrijk als in het buitenland).[279] Dit doet MI5 door de verzameling van binnenlandse inlichtingen ten behoeve van verschillende overheidsinstanties, met inbegrip van opsporingsdiensten. Daarnaast geeft MI5 advies en begeleiding aan andere overheidsinstanties en bedrijven op het gebied van veiligheid. MI5 valt onder de verantwoordelijkheid van de Minister van Binnenlandse Zaken (de *Home Secretary*).

De belangrijkste taken van MI5 zijn:

1. De bescherming van de nationale veiligheid tegen diverse dreigingen, waaronder terrorisme, spionage, sabotage, economische dreigingen, massavernietigingswapens,

[275] Zie bijvoorbeeld Weaver 2024, p. 90 en Jalalzai 2016, p. 9.
[276] Leigh 2019, p. 555.
[277] Leigh 2023, p. 4; Weaver 2024, p. 90. Er is ook nog de Defence Intelligence, een afdeling van het Ministerie van Defensie; een all-source dienst die niet onafhankelijk is, zoals MI5, SIS en GCHQ. Zie: 'Defence Intelligence', gov.uk. Deze dienst blijft buiten beschouwing in dit hoofdstuk.
[278] Cabinet Office & National Security and Intelligence, *National Intelligence Machinery Booklet*, gov.uk, 19 november 2010.
[279] Leigh 2019, p. 560.

cyberaanvallen, activiteiten van statelijke actoren en acties gericht op ondermijning van de parlementaire democratie.
2. De bescherming van het economische welzijn van het Verenigd Koninkrijk.
3. Het ondersteunen van de activiteiten van de politiediensten en andere handhavingsinstanties bij het voorkomen en opsporen van ernstige criminaliteit.[280]

De bevoegdheden van MI5 zijn vastgelegd in de Intelligence Services Act 1994, de Security Service Act 1989, de RIPA 2000, de Investigatory Powers Act 2016 (hierna: IPA 2016), en de Investigatory Powers Act 2024 (hierna: IPA 2024). De voornaamste manieren van inlichtingenverzameling zijn: het onderscheppen van communicatie (gericht en in bulk), het verzamelen en verwerken communicatiegegevens, gerichte surveillance (met behulp van camera's of microfoons), en de inzet van een hackbevoegdheid.[281]

### 6.1.2 SIS (MI6)

SIS, ook wel 'MI6' genoemd, is de Britse inlichtingendienst buitenland. SIS verzamelt buitenlandse inlichtingen ter ondersteuning van het veiligheids-, defensie-, buitenlands en economisch beleid van de regering, met als doel Britse burgers te beschermen tegen overzeese dreigingen. Daartoe voert SIS diverse activiteiten uit, zoals spionage en heimelijke acties. SIS legt een sterke nadruk op *human intelligence* (HUMINT) en *technical intelligence* (TECHINT). SIS valt onder het Ministerie van Buitenlandse Zaken (de *Foreign Secretary)*.[282]

De belangrijkste taken van SIS zijn:

1. Terrorismebestrijding: zowel met betrekking tot het voorkomen en tegenhouden van terroristische aanvallen in het Verenigd Koninkrijk, als aanvallen tegen overzeese belangen van het VK en haar bondgenoten.
2. Bestrijding van dreigingen van vijandige statelijke actoren, het bevorderen van de welvaart van het Verenigd Koninkrijk en het onderhouden van internationale betrekkingen.
3. Het beschermen en bevorderen van het cyberdomein van het VK.[283]

### 6.1.3 GHCQ

De GHCQ is de Britse communicatie-inlichtingendienst en nationale SIGINT organisatie. Het richt zich op SIGINT en heeft net als de SIS een focus op het buitenland.[284] GCHQ speelt ook een belangrijke rol bij het beschermen van vitale infrastructuren, zoals energie-, water- en communicatienetwerken. Op dit gebied werkt de GCHQ nauw samen met MI5.[285] GCHQ valt

[280] MI5 noemt de drie taken: 1. 'Countering Terrorism', 2. 'Countering State Threats' en 3. 'Protective Security'. Zie 'How we work', 'Law, oversight and ethics', en 'What we do', *mi5.gov.uk* (laatst geraadpleegd op 21 juli 2025). Zie ook: Leigh 2019, p. 560; Leigh 2023, p. 4; Weaver 2024, p. 90. De functies van MI5 zijn vastgelegd in de Security Service Act 1989.
[281] 'How we work', 'Law, oversight and ethics', 'Gathering intelligence', *mi5.gov.uk* (laatst geraadpleegd op 21 juli 2025).
[282] 'Is MI5 a government department?' en 'What is the difference between MI5 and MI6 (SIS)?' (FAQ), *mi5.gov.uk*; 'SIS (MI6) at a glance' (video), *sis.gov.uk* (laatst geraadpleegd op 21 juli 2025); Leigh 2023, p. 4; Weaver 2024, p. 90.
[283] 'About us', *sis.gov.uk* (laatst geraadpleegd op 21 juli 2025). De functies van SIS zijn vastgelegd in section 1 van de Intelligence Services Act 1994.
[284] 'Legal framework', *gchq.gov.uk* (laatst geraadpleegd op 21 juli 2025).
[285] Cabinet Office & National security and intelligence 2010, p. 8.

net als SIS onder de verantwoordelijkheid van het Ministerie van Buitenlandse Zaken (de *Foreign Secretary*).[286]

De belangrijkste taken van GCHQ zijn:

1. Terrorismebestrijding: zowel in het Verenigd Koninkrijk als van overzeese belangen.
2. Cyber Security: met als missie: 'het VK de veiligste plaats maken om online te leven en zaken te doen'.
3. Het behouden en beschermen van strategisch voordeel door dreigingen van vijandige staten aan te pakken, het economisch welzijn te beschermen en internationale betrekkingen te onderhouden.
4. De bestrijding van ernstige en georganiseerde misdaad.
5. Het ondersteunen van defensie door defensiepersoneel en -goederen te beschermen en een geïntegreerde aanpak van oorlogsvoering te stimuleren.[287]

### 6.1.4 National Cyber Security Centre (NCSC)

Het *National Cyber Security Centre* (NCSC) werd in 2016 opgericht om verschillende kerntaken met betrekking tot cyberspace samen te brengen.[288] Vooral de informatievoorziening werd door bedrijven als versnipperd en verwarrend ervaren. Gelet op de uitgebreide kennis en expertise binnen GCHQ, achtte het Verenigd Koninkrijk het logisch om het NCSC daar onder te plaatsen.[289]

Het NCSC houdt zich bezig met het beschermen van de vitale infrastructuur in het VK tegen cyberaanvallen.[290] Het fungeert als een 'brug' tussen de overheid en bedrijven, en biedt een centrale bron van informatie, advies en begeleiding.[291] Het NCSC werkt nauw samen met wetenschappers, bedrijven en andere overheidsinstanties, zoals opsporingsdiensten, inlichtingendiensten, en internationale partners.[292]

## 6.2 De uitoefening van bulkinterceptie in het Verenigd Koninkrijk

De uitoefening van bulkinterceptie en andere onderzoeksbevoegdheden van Britse overheidsinstanties, evenals het toezicht op deze bevoegdheden, wordt geregeld door de volgende wetten:

1. Regulation of Investigatory Powers Act 2000 (RIPA);
2. Investigatory Powers Act 2016 (IPA 2016);
3. Investigatory Powers (Amendment) Act 2024.

Deze wetten, die 'statute law' genoemd worden, zijn afkomstig van het Britse parlement en vormen de 'primary legislation', waarin de basisprincipes van de wetgeving zijn vastgelegd. Ze gelden doorgaans voor het gehele Verenigd Koninkrijk.[293] De details worden verder

---

[286] 'Is MI5 a government department?', *mi5.gov.uk* (laatst geraadpleegd op 21 juli 2025).
[287] 'Our mission. Overview', *gchq.gov.uk* (laatst geraadpleegd op 21 juli 2025). De functies van GCHQ zijn vastgelegd in s.3 van de Intelligence Services Act 1994.
[288] Zie *Ncsc.gov.uk*.
[289] 'Chancellor's speech to GCHQ on cyber security', *gov.uk*, 17 november 2015 (laatst geraadpleegd op 21 juli 2025); Hannigan 2019, p. 14.
[290] 'About us', *gchq-careers.co.uk* (laatst geraadpleegd op 21 juli 2025).
[291] 'National Cyber Security Centre', *gov.uk* (laatst geraadpleegd op 21 juli 2025).
[292] 'NCSC Launch Video', *ncsc.gov.uk* (laatst geraadpleegd op 21 juli 2025).
[293] Het precieze geografische bereik staat aan het begin van iedere Act (zie ook Partington 2021, p. 33-34).

uitgewerkt in ‘secondary legislation’, ook wel ‘statutory instruments’ genoemd, zoals de *Investigatory Powers Tribunal Rules 2018*.[294] Daarnaast bestaat er nog ‘tertiary legislation’ en ‘quasi-legislation’ of ‘soft law’, zoals *Codes of Practice*. Hoewel deze documenten belangrijke richtlijnen bieden, vormen ze strikt genomen geen wetgeving.[295]

De RIPA 2000 vormde de eerste stap in de regulering van heimelijke bevoegdheden van Britse overheidsinstanties. Het primaire doel was het in overeenstemming brengen van onderzoeksbevoegdheden met mensenrechten, zoals beschreven in het EVRM.[296] De IPA 2016 had tot doel bestaande bevoegdheden te verduidelijken en samen te voegen in één wet, waardoor het toezicht op en de waarborgen rondom deze bevoegdheden werden verbeterd. Bovendien werd de wetgeving gemoderniseerd, omdat de RIPA 2000 niet voldoende was om de technologische ontwikkelingen bij te benen.[297]

### 6.2.1 De ontwikkelingen n.a.v. *Big Brother Watch*

Zoals in paragraaf 2.1.1 is aangegeven, werd het Verenigd Koninkrijk door het EHRM veroordeeld voor schending van artikel 8 EVRM vanwege het gebruik van bulkinterceptie. De belangrijkste tekortkoming in het Britse systeem betrof het ontbreken van voorafgaande toestemming voor het selecteren van gegevens uit bulkinterceptie.

De RIPA 2000 bevatte alleen bepalingen over interceptie in het algemeen; met de IPA 2016 werd een onderscheid geïntroduceerd tussen reguliere (gerichte) interceptie en bulkinterceptie.[298] De *Interception of Communication Code of Practice* noemt uitsluitend MI5, SIS en GCHQ als bevoegde autoriteiten voor de bulkinterceptie.[299] Deze drie inlichtingendiensten kunnen aanvragen indienen voor bulkinterceptie. In de praktijk lijkt dit vooral GCHQ te zijn, vermoedelijk vanwege hun specialisatie in SIGINT en focus op dreigingen buiten het Verenigd Koninkrijk.[300]

De *Investigatory Powers Commissioner’s Office* (IPCO) werd op 1 september 2017 opgericht als gevolg van de Investigatory Powers Act 2016. Deze wet werd mede ingegeven door zorgen over het gebrek aan transparantie en toezicht op de Britse inlichtingen- en veiligheidsdiensten,

---

[294] De Investigatory Powers Tribunal Rules 2018 zijn op 31 december 2018 in werking getreden. Ze vervingen de Investigatory Powers Tribunal Rules 2000. Primaire en secundaire wetgeving, evenals de toelichting (*Explanatory Notes*) op die wetten, zijn terug te vinden op *legislation.gov.uk*. Er zijn twee versies raadpleegbaar: ‘Original (As enacted)’ en ‘Latest available (Revised)’. In het onderzoek voor dit hoofdstuk is steeds de laatste versie geraadpleegd.

[295] Partington 2021, p. 34. De bevoegdheid van de minister om *Codes of Practice* uit te vaardigen staat in de RIPA, artikel 71 *“(1) The Secretary of State shall issue one or more codes of practice relating to the exercise and performance of the powers and duties mentioned in subsection (2)”* en zie de Explanatory Notes bij de RIPA 2000, nr. 15.

[296] Explanatory Notes bij de RIPA 2000, ‘Summary and Background’, nr. 3.

[297] ‘What were the policy objectives of the measure?’ en ‘Post Implementation Review IPA 2016’, *gov.uk*, 28 april 2023 (laatst geraadpleegd op 21 juli 2025). Lord David Anderson’s rapport uit 2015 vormde de blauwdruk voor de IPA 2016. Voorafgaand aan de actualisering in 2024 heeft Anderson in opdracht van de Home Office een evaluatie uitgevoerd. Daarin heeft hij (voornamelijk m.b.t. bulkbevoegdheden en *bulk personal datasets* (*BPDs*)) beoordeeld of en wat er in de IPA 2016 moest worden herzien (zie Anderson, 2015; 2016; en 2023).

[298] Dat is geregeld in Part 6, Chapter 1 van de IPA 2016. Explanatory Notes bij de IPA 2016, ‘Legal background’, nr. 15. De IPA-bepalingen m.b.t. gerichte interceptiebevelen en bulkinterceptie vervingen de interceptie-bepalingen in s.8(1) en (4) van de RIPA 2000. Zie ook het IPCO Jaarrapport 2017, pt. 7.1, p. 40.

[299] § 4.8 van de Code of Practice (§ 2.27 in de nieuwe Code of Practice).

[300] Deze conclusie wordt ondersteund door bijvoorbeeld het *IPCO Annual Report 2022* waarin gedetailleerd per dienst staat uitgeschreven welke bevoegdheden ze hebben gebruikt; bij GCHQ staat onder een aparte kop ‘Bulk Interception’, bij MI5 en SIS niet. Zie ook Leigh 2019, p. 560.

zoals naar voren kwam in de nasleep van de Snowden-onthullingen en de zaak die werd aangespannen door *Big Brother Watch e.a.*. Deze gespecialiseerde toezichtsinstantie houdt ook toezicht op de inzet van onderzoeksbevoegdheden van Britse inlichtingen- en veiligheidsdiensten, waaronder bulkinterceptie.

### 6.2.2 Ex ante toestemming

Een aanvraag voor bulkinterceptie moet primair gericht zijn op het onderscheppen van communicatie afkomstig van buiten het Verenigd Koninkrijk ('overseas-related communications') of de "secundaire gegevens" die hiermee verband houden.[301] Met overzeese communicatie wordt verstaan communicatie die verzonden of ontvangen is buiten de Britse eilanden.[302] De aanvraag moet gedetailleerd uiteenzetten wat de specifieke operationele doelen van de bulkinterceptie zijn.[303] De mogelijk doelen voor bulkinterceptie zijn:

1. De bescherming van de nationale veiligheid.
2. Het voorkomen of opsporen van ernstige criminaliteit.
3. Het economisch welzijn van het VK (mits ook in het belang voor de nationale veiligheid).
4. Het uitvoering geven aan een rechtshulpverzoek.[304]

Voor het verzamelen van gegevens door middel van bulkinterceptie moet de proportionaliteit en subsidiariteit worden getoetst, door de volgende elementen af te wegen: (a) kan het beoogde doel ook met minder ingrijpende middelen kan worden bereikt?; (b) de mate van gevoeligheid van de gegevens; (c) het algemeen belang van de integriteit en veiligheid van telecommunicatiesystemen en postdiensten; en (d) andere 'aspecten van het algemeen belang', zoals de bescherming van de persoonlijke levenssfeer.[305] De aanvraag voor bulkinterceptie omvat tevens een aanvraag voor de selectie van gegevens voor onderzoek. Voor deze selectie geldt eveneens een toets op noodzakelijkheid en proportionaliteit. Naar aanleiding van de uitspraak in *Big Brother Watch e.a.* heeft GCHQ een extra waarborg ingebouwd in het autorisatieproces: 'strong selectors' moeten nu worden goedgekeurd door een senior GCHQ-medewerker.[306]

De minister (*Secretary of State*) kan, namens een inlichtingendienst, besluiten om de bevoegdheid tot bulkinterceptie in te zetten.[307] De aanvragen van de minister voor het gebruik van deze (en andere) onderzoeksbevoegdheden moeten vooraf worden goedgekeurd door een 'Judicial Commissioner' van de IPCO. Dit "double-lock systeem" werd ingevoerd door de IPA 2016.[308] Alleen na deze bekrachtiging mag de bevoegdheid worden uitgeoefend; het oordeel

[301] s.136(3) IPA 2016. Section 137 beschrijft de categorie van 'secondary data'. Secondaire gegevens geven, indien gescheiden van de communicatie, geen informatie over de inhoud van de communicatie.
[302] s.136(3) IPA 2016 en IPCO Jaarrapport 2017, pt. 7.8, p. 41.
[303] In s.142 en § 6.20 van de Code of Practice wordt beschreven welke informatie moet worden vermeld in een bulkinterceptiebevel.
[304] Explanatory Notes bij de IPA 2016, 'Commentary on provisions of Act', nr. 399 en § 4.11 Code of Practice.
[305] s.2(2) IPA 2016 en § 4.15 en 4.16 van de Code of Practice.
[306] IPCO Annual Report 2022, § 3.7, p. 16.
[307] s.138 (1) IPA 2016.
[308] Het double-lock systeem geldt ook voor sommige andere ingrijpende bevoegdheden, zoals observatiebevelen (zie Klein 2023). In sommige gevallen is er een zogenoemd "triple-lock systeem", waarbij ook de Britse premier (*Prime Minister*) moet tekenen. Dit is bijvoorbeeld in het geval van gerichte interceptie jegens een lid van het Britse parlement (s.26 IPA 2016 en de Explanatory Notes bij de IPA 2016, 'Commentary on provisions of Act', nr. 376).

van de IPCO is dus bindend. De goedkeuring of afkeuring van de Judicial Commissioner wordt schriftelijk gemotiveerd, zodat de aanvrager het verzoek kan heroverwegen.[309]

De Judicial Commissioner toetst het bevel dus op criteria van noodzakelijkheid en proportionaliteit, waarbij ook het doel van het bevel en eventuele overwegingen met betrekking tot buitenlandse operatoren in acht worden genomen.[310] De aanvragende instantie is verplicht om de IPCO te voorzien van alle informatie die nodig is voor een weloverwogen oordeel.[311]

### 6.2.3 Ex durante toezicht

De IPCO kondigde in het jaarrapport van 2022 aan dat het aandacht zal besteden aan technologische ontwikkelingen waarmee (de selectie van data verkregen door) bulkinterceptie meer geautomatiseerd (en *ex durante*) kan worden uitgevoerd, en bulkinterceptie potentieel ook gerichter (en daardoor proportioneler) kan worden uitgevoerd.[312]

Onder de 'Data assurance programme' controleren inspecteurs of systemen automatisch loggen wie toegang heeft tot gegevens, of deze toegang rechtmatig is, en of er voldoende technische en organisatorische waarborgen zijn om misbruik te voorkomen. Deze logging wordt actief gecontroleerd tijdens inspectiebezoeken, waarbij ook steekproeven worden genomen.[313]

De IPCO benadrukt dat het toezicht niet alleen handmatig gebeurt, maar ook via geautomatiseerde controlesystemen die door de diensten zelf worden gebruikt. Tijdens inspecties wordt geëvalueerd of deze systemen effectief zijn in het signaleren van ongeautoriseerde toegang of afwijkend gedrag. Daarnaast voert IPCO *compliance-audits* uit op datasets, waarbij wordt gekeken naar de rechtmatigheid van verzamelde gegevens, de duur van opslag, en de naleving van verwijderingsprotocollen. Deze audits zijn er om te waarborgen dat de verwerking van gegevens in overeenstemming is met de Investigatory Powers Act 2016.[314]

### 6.2.4 Ex post toezicht

De IPCO voert ook ex post toezicht uit door middel van inspecties uit om te controleren of de inlichtingendiensten voldoen aan de wet- en regelgeving en de Code of Practice. Een typische inspectie bestaat uit verschillende evaluatiestappen, zoals het beoordelen of bevelen voldeden aan de vereisten van noodzakelijkheid en proportionaliteit, het uitvoeren van interviews met betrokken medewerkers, en controles op de naleving van procedurevoorschriften. Daarbij wordt ook gekeken naar de toereikendheid van die procedures om herhaling van fouten te voorkomen. Van elke inspectie wordt een rapport opgemaakt, waarin de bevindingen worden beschreven en aanbevelingen voor verbetering worden gedaan. Deze rapporten worden verzonden naar het hoofd van de betreffende inlichtingendienst en de minister.[315]

---

[309] s.140 IPA 2016 en zie Explanatory Notes bij de IPA 2016, 'Commentary on provisions of Act', nrs. 407-410.
[310] s.138(1)(g) IPA 2016, § 6.28 Code of Practice en zie ook de tabel over de noodzakelijke autorisatie per bevoegdheid op de website van de IPCO: 'The powers' en 'Authorisations', *ipco.org.uk* (laatst geraadpleegd op 21 juli 2025).
[311] § 6.29 Code of Practice.
[312] IPCO Annual Report 2022, § 10.15, p. 47.
[313] IPCO Annual Report 2022, p. 36-38.
[314] IPCO Annual Report 2022, p. 39-41.
[315] IPCO Annual Report 2017, § 7.38, p. 46 en § 7.46-7.48, p. 47.

De Code of Practice specificeert verder de elementen die onderdeel moeten zijn van een inspectie. Het inspectieteam bestaat daarbij uit verschillende specialisten. Bij inspecties met betrekking tot bulkinterceptie is er bijvoorbeeld altijd een Judicial Commissioner en een lid van de 'Technology Advisory Panel' (TAP) aanwezig.[316]

### 6.2.5 Effectief rechtsmiddel

In de *Big Brother Watch*-uitspraken toonde het EHRM al tevredenheid over het 'robuuste rechtsmiddel' dat geboden wordt door het bestaan van de Investigatory Powers Tribunal (IPT).

De IPT is een speciale rechtbank die is ingesteld voor de behandeling van klachten van burgers over vermeend onrechtmatig handelen door Britse inlichtingendiensten op basis van de RIPA. Het is bevoegd om deze klachten te onderzoeken, kennis te nemen van staatsgeheime informatie en relevante documentatie bij de diensten op te vragen. Indien een schending van de RIPA wordt vastgesteld, kan de IPT een schadevergoeding toewijzen en het bevel geven tot vernietiging van gegevens als gevolg van het onrechtmatige handelen (zie verder paragraaf 6.3.2).

## 6.3 Het stelsel van toezicht

Deze paragraaf beschrijft het bredere toezichtstelsel op de inlichtingen- en veiligheidsdiensten in het Verenigd Koninkrijk. Ook worden de 'overige toezichthouders', zoals de parlementaire toezichthouders en nationale rekenkamers, kort beschreven.

### 6.3.1 IPCO

De IPCO in 2016 is ingesteld om begrip en vertrouwen in het toezicht op onderzoeksbevoegdheden van de overheid te bevorderen, en om de wijze waarop deze bevoegdheden worden ingezet, te verantwoorden.[317] Op 1 september 2017 werd de IPCO operationeel. Daarbij werden de toezichtfuncties van drie voorgangers verenigd in één instantie.[318] In totaal werkten er in 2024 bij de IPCO ongeveer 150 inspecteurs, juristen en beleidsmedewerkers.[319]

De IPCO bestaat uit de *Investigatory Powers Commissioner*, ondersteund door een team van Judicial Commissioners[320], de Chief Executive Officer (voorzitter) en het TAP. De judicial commissioners zijn recent gepensioneerde rechters van een High Court, een Court of Appeal of de Supreme Court. De wijze waarop de IPC en de overige commissioners worden voorgedragen en aangesteld, evenals de voorwaarden waaraan zij moeten voldoen, staan beschreven in de Investigatory Powers Act 2016 (section 227). Daarin staat bijvoorbeeld dat alleen door bepaalde personen unaniem een persoon mag worden voorgedragen en aangesteld,

[316] Toelichting door de CEO en twee adviseurs van IPCO tijdens het gesprek op 8 april 2025.
[317] 'Investigatory Powers Act 2016 (IPA 2016) Post Implementation Review 2024', 'Oversight', *gov.uk*, 28 april 2023; 'Investigatory Powers (Amendments) Bill Oversight and Safeguards', *gov.uk*, 26 april 2024 (laatst geraadpleegd op 21 juli 2025).
[318] Die voorgangers waren: de 'Office of the Surveillance Commissioners', de 'Interception of Communications Commissioner's Office' en de 'Intelligence Service Commissioner'. Zie *IPCO Jaarrapport 2017*, p. 8.
[319] Zie Who we are - IPCO, *ipco.org.uk* (laatst geraadpleegd op 21 juli 2025).
[320] Bij de start in 2017 waren er 16 Judicial Commissioners. In 2025 zijn dat er 13, inclusief de Investigatory Powers Commissioner (er staan 13 biografieën op de pagina Who we are - IPCO, *ipco.org.uk* (laatst geraadpleegd op 21 juli 2025).

en dat de voorgedragen persoon van 'high judicial office' moet zijn, oftewel een senior of recent gepensioneerde rechter.[321]

De aanbeveling van Anderson om de TAP (*Technology Advisory Panel*) in te stellen, is opgevolgd bij de inwerkingtreding van de IPA 2016. De TAP kan niet zelfstandig beslissen, maar levert (onafhankelijk) advies aan de IPCO en de Judicial Commissioners over de impact van de technologieën die gebruikt worden bij de onderzoeksbevoegdheden, om zo de inbreuk op de privacy zo klein mogelijk te houden. Ook kan de TAP de minister adviseren als die daar om vraagt. Naast het specifieke toezicht houdt de TAP zich ook bezig met overkoepelende vraagstukken, zoals de vraag hoe de publieke instanties waarop toezicht wordt gehouden omgaan met AI, en hoe dat het werk van IPCO beïnvloedt.

De IPCO houdt toezicht op meer dan 600 instanties die onderzoeksbevoegdheden mogen toepassen, zoals opsporingsdiensten en inlichtingendiensten, maar ook penitentiaire inrichtingen en andere instanties.[322] Het toezicht op bulkinterceptie vormt slechts een klein onderdeel van hun werkzaamheden. Voor zover er toezicht is op het NCSC, verloopt dat altijd via GCHQ, evenals de aanvragen voor de inzet van bulkinterceptie zelf, aangezien het NCSC geen aparte instantie is, maar een onderdeel van GCHQ.[323]

De IPCO beschikt over eigen bevoegdheden om hun taak uit te voeren en de diensten zijn verplicht om inzage te geven in alle informatie en documenten die daarvoor noodzakelijk zijn.[324]

De IPCO publiceert rapporten om het parlement en de samenleving te informeren over haar werkzaamheden. Aan de *Prime Minister* wordt in ieder geval jaarlijks een rapport overhandigd. De Prime Minister is verplicht om de jaarrapporten van de IPC te publiceren, waarbij tevens wordt vermeld of er informatie geheim wordt gehouden. Deze jaarrapporten zijn uitvoerig en gedetailleerd, inclusief statistieken met betrekking tot bijvoorbeeld het aantal ingediende aanvragen, door welke instantie, en het aantal goed- en afkeuringen van bijzondere bevoegdheden door IPCO.[325] In het kader van transparantie is de IPCO verplicht om "serious errors" te melden (mits in het algemeen belang is om die gegevens bekend te maken) aan de betrokken partijen, zodat zij de mogelijkheid hebben om een klacht in te dienen bij de IPT.[326]

Opvallend is de sterke (door de IPCO zelf omschreven als 'symbiotische') verhouding tussen de verschillende fases van toezicht binnen één orgaan: de Judicial Commissioners van de IPCO hebben de verantwoordelijkheid om vooraf aanvragen voor inzet van bevoegdheden te keuren, en de inspecteurs houden tijdens en achteraf toezicht. In veel landen zijn deze functies van elkaar gescheiden in verschillende instanties. Volgens de IPCO is deze vereniging van

[321] Er staan 13 biografieën van Judicial Commissioners op de website. 'Who we are', ipco.org.uk; Leigh 2023, p. 4.
[322] 'Organisations we oversee', *ipco.org.uk* (laatst geraadpleegd op 21 juli 2025).
[323] Toelichting door de CEO en twee adviseurs van IPCO tijdens het gesprek op 8 april 2025.
[324] *IPCO Annual report 2017*, § 2.5-2.6 p. 9; 'Investigatory Powers (Amendments) Bill Oversight and Safeguards', gov.uk, 26 april 2024; Leigh 2023, p. 5.
[325] s.234(6) IPA 2016. De jaarrapporten worden gepubliceerd op de website van IPCO, ipco.org.uk, en zie: 'Investigatory Powers (Amendments) Bill Oversight and Safeguards', gov.uk, 26 april 2024.
[326] Leigh 2019, p. 577; *IPCO Annual report 2017*, p. 8 en § 14.2, p. 90. De definitie van 'error' staat in s.231(9) IPA.

toezichtfases in één instantie bevorderend voor de kwaliteit van het algehele toezicht op onderzoeksbevoegdheden.[327]

### 6.3.2 IPT

De *Investigatory Powers Tribunal* (IPT) is een onafhankelijke rechtbank die is opgericht met de RIPA 2000. In deze wet staan de rechtsmacht en de bevoegdheden van de IPT beschreven. De IPT heeft als enige rechtbank jurisdictie in het gehele Verenigd Koninkrijk: zowel in Schotland, Noord-Ierland, Engeland en Wales. De IPT is onafhankelijk en bestaat uit senior rechters die worden aangesteld door de Britse koning.[328] In de RIPA 2000 zijn ook de *Investigatory Powers Tribunal Rules* (hierna: de Rules) opgesteld.[329] Die bevatten de regels met betrekking tot de procedures voor de IPT.

De primaire doelstelling van de IPT is om te waarborgen dat onderzoeksbevoegdheden in overeenstemming met de wet worden toegepast. Daarnaast behandelt de IPT klachten over het gedrag van, of namens, de inlichtingendiensten, ongeacht of deze klachten betrekking hebben op het gebruik van onderzoeksbevoegdheden.[330] Een andere belangrijke taak is het bieden van een effectief rechtsmiddel voor belanghebbenden. De IPT is de enige rechtbank die bevoegd is om klachten en procedures tegen de inlichtingendiensten te behandelen.[331] De IPT heeft de plicht om klachten te onderzoeken, tenzij er sprake is van een van de weigeringsgronden.[332] Klagers hoeven niet zelf bewijs aan te leveren voor hun klacht: zij zetten alleen uiteen wat er volgens hen is gebeurd, waarna de IPT de feiten onderzoekt.[333]

De RIPA 2000 verplicht de inlichtingendiensten tot medewerking en het verstrekken van relevante documenten en informatie aan de IPT.[334] De IPT houdt openbare zittingen voor zover dat mogelijk is. Soms moet is het besloten kring in het belang van de nationale veiligheid en er bijvoorbeeld staatgeheim materiaal wordt besproken.[335]

Zoals is aangegeven in paragraaf 2.1.1 en 6.2.5, kan de IPT bindende beslissingen nemen, zoals het geven van de opdracht tot het stopzetten van een operatie, het vernietigen van materiaal, en het toekennen van een schadevergoeding.[336] Onder de IPA 2016 werd een beperkte vorm van hoger beroep mogelijk gemaakt naar aanleiding van uitspraken van de IPT (*on a point of law).*[337] Met andere woorden, als naar mening van een appellant een beslissing van het IPT

[327] IPCO Annual Report 2017, § 2.11, p. 10.
[328] Explanatory Notes bij de IPA 2016, § 7.5, p. 2.
[329] Op basis van s.69 kan de Secretary of State *rules* opstellen waarvoor geen goedkeuring van het parlement nodig is. De Investigatory Powers Tribunal Rules 2018 zijn op 31 december 2018 in werking getreden.
[330] IPT Report 2016-2021, p. 7.
[331] Daarnaast kan de IPT ook klachten over andere publieke organen, zoals de politie, in behandeling nemen. Zie: s.65 RIPA 2000 en s.7 Human Rights Act 1998; 'How the Tribunal Works', in: *IPT Report 2016-2021,* p. 38; 'Complaints the Tribunal can consider'*, investigatorypowerstribunal.org.uk* (laatst geraadpleegd op 21 juli 2025).
[332] De meerderheid van de klachten buiten de jurisdictie van de IPT, of waren *vexatious* of *frivolous*, waardoor ze niet in behandeling werden genomen (IPT Report 2016-2021, p. 38). Zie ook Leigh 2019, p. 577 en 2023, p. 6.
[333] IPT Report 2016-2021, p. 4.
[334] s.68(6) RIPA; 'How the Tribunal Works', in: *IPT Report 2016-2021,* p. 36.
[335] IPT Report 2016-2021, p. 4.
[336] IPT Report 2016-2021, p. 36. Leigh 2019, p. 576.
[337] De IPT verwijst in het IPT Report 2016-2021, p. 13, naar de uitspraak van de Supreme Court in de zaak van *R (on the application of Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22, waarin werd geoordeeld dat s.67(8) IPA 2016 de High Court niet uitsluit.

gebaseerd is op een verkeerde interpretatie of toepassing van de wet, dan kan die fout door een hogere rechtbank worden gecontroleerd.

### 6.3.3 De verhouding tussen IPCO en IPT

IPCO en IPT hebben verschillende, maar elkaar aanvullende functies, en op een aantal vlakken werken ze met elkaar samen.[338] Zo ontmoeten de hoofden van IPCO en IPT elkaar jaarlijks en kan de IPT voor zover nodig inspecteurs 'lenen' van de IPCO. De IPCO is wettelijk verplicht om ondersteuning te bieden wanneer de IPT daarom vraagt, en alle benodigde documenten en informatie aan de IPT te verstrekken. Omgekeerd moet de IPT de IPCO op de hoogte houden van alle procedures en klachten die bij haar worden ingediend, evenals de uitkomst van elke zaak.[339]

Ondanks deze nauwe band zijn IPCO en IPT twee afzonderlijke instanties met elk hun eigen rol en taken. De IPT biedt een arbitragemechanisme voor conflictbeslechting (achteraf) en functioneert in die zin als een rechtbank. De IPCO is een specialistische toezichthouder en beoordeelt de wettigheid van bevelschriften en de naleving van andere relevante wetgeving, waarbij het beslechten van een mogelijk conflict niet centraal staat.[340] De IPCO heeft geen bevoegdheid om klachten in behandeling te nemen en verwijst klachten daarom door naar het IPT, zonder zelf verdere actie te ondernemen.[341] Het is daarom mogelijk dat een bevel voor de inzet van een bevoegdheid wordt goedgekeurd door een judicial commissioner van de IPCO, wordt aangevochten bij het IPT en de inzet achteraf alsnog onrechtmatig wordt bevonden.

### 6.3.4 Overige toezichthouders

Deze paragraaf beschrijft de overige instanties die een rol spelen in het controleren van de Britse inlichtingen- en veiligheidsdiensten. De nadruk ligt in dit rapport op het rechtmatigheidstoezicht. Deze instanties worden om deze reden slechts kort omschreven.

*De nationale rekenkamer*

De *National Audit Office* (NAO) controleert de overheidsuitgaven, waaronder ook de uitgaven van inlichtingen- en veiligheidsdiensten in het Verenigd Koninkrijk.[342] De controle op deze uitgaven vindt plaats op basis van afspraken met de 'Controller and Auditor General'. Vanwege veiligheidsredenen worden de auditresultaten en rapporten van de NAO over deze diensten niet openbaar gemaakt, maar rechtstreeks overhandigd aan de voorzitter van de 'Public Accounts Committee'. Vervolgens vindt een nadere beoordeling plaats binnen het ISC.[343]

*Parlementair toezicht*

De *Intelligence and Security Committee* (hierna: ISC) is een commissie van negen parlementariërs, afkomstig uit zowel het 'House of Commons' als het 'House of Lords'.[344] De ISC houdt parlementair toezicht op het beleid, de uitgaven, de administratie en de operaties

[338] IPCO Annual Report 2017, § 15.1, p. 106.
[339] s.68 RIPA en s.232 IPA 2016; IPCO Annual Report 2016, § 15.4, p. 106; IPT Report 2016-2021, 'Relationship between Tribunal and IPC', p. 9.
[340] IPT Report 2016-2021, p. 4.
[341] Toelichting door de CEO en twee adviseurs van IPCO tijdens het gesprek op 8 april 2025.
[342] Zie Home - National Audit Office (NAO) (laatst geraadpleegd op 21 juli 2025).
[343] Dawson & Godec 2017, p. 54.
[344] Leigh 2019, p. 572. De ISC werd opgericht met de Intelligence and Services Act 1994, en is hervormd door de Justice and Security Act 2013.

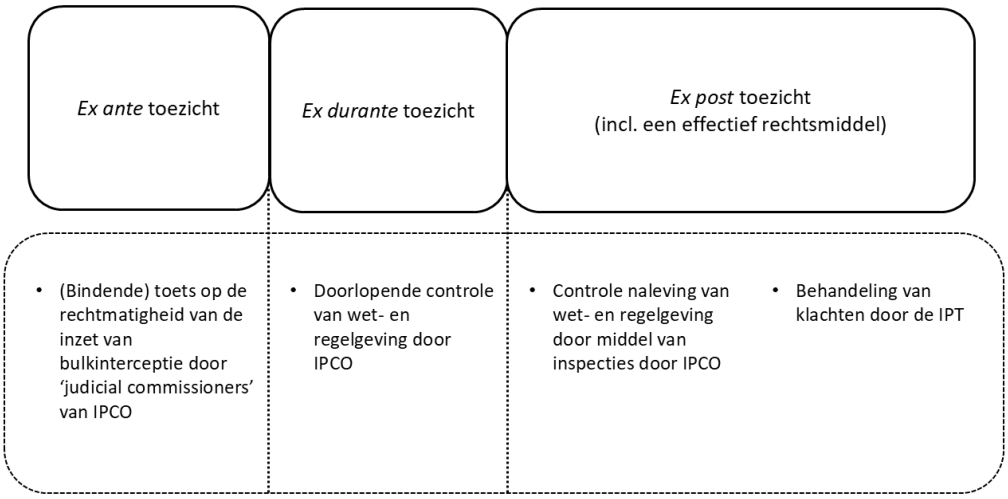
van MI5, MI6, GCHQ, Defence Intelligence, de National Cyber Force, de Joint Intelligence Organisation, het National Security Secretariat en de Homeland Security Group.[345]

De ISC houdt geen toezicht op de operationele activiteiten van de diensten. Wel controleert de ISC de lijst van 'operational purposes' bij bulkinterceptie en heeft de IPC de bevoegdheid om zaken door te sturen naar de IPCO voor onderzoek, inspectie of controle.[346] In 2015 deed de ISC bijvoorbeeld onderzoek naar de 'intrusive capabilities' die de Britse inlichtingen- en veiligheidsdiensten gebruiken. GCHQ's gebruik van bulkinterceptie werd onder de loep genomen, waarna de ISC tot de conclusie kwam dat slechts een klein deel van het internetverkeer wordt verzameld met deze bevoegdheden, dat nog kleinere delen worden doorzocht met geautomatiseerde middelen, en dat slechts een zeer klein deel hiervan ooit zal worden gelezen door een menselijke analist.[347]

## 6.4 Conclusie

In het Verenigd Koninkrijk zijn verschillende inlichtingen- en veiligheidsdiensten bevoegd aanvragen in te dienen voor bulkinterceptie. In de praktijk dient de GCHQ als SIGINT-organisatie de meeste aanvragen in en voert deze de meeste operaties uit. De wetgeving omtrent bulkinterceptie en het bijbehorende toezicht is aanzienlijk geëvolueerd, mede als gevolg van de Snowden-onthullingen en de veroordelingen van het Verenigd Koninkrijk in de Big Brother Watch-zaken.

De RIPA 2016 consolideerde de bevoegdheden van opsporingsinstanties en inlichtingen- en veiligheidsdiensten in één wet en moderniseerde zowel de bevoegdheden als het toezichtstelsel. Het stelsel van toezicht ten aanzien van bulkinterceptie in het Verenigd Koninkrijk is weergegeven in Figuur 5.




Figuur 5: Het stelsel van toezicht ten aanzien van bulkinterceptie in het Verenigd Koninkrijk

[345] Zie *isc.independent.gov.uk*; Leigh 2019, p. 556 en 572.
[346] Wettelijk vastgelegd in s.142(8) IPA 2016. Leigh 2019, p. 567; Leigh 2023, p. 5.
[347] Zie Intelligence and Security Committee of Parliament, 'Privacy and Security: A modern and transparent legal framework', *isc.independent.gov.uk,* 2015, p. 31-32; Leigh 2019, p. 564.

De IPCO fungeert als de onafhankelijke, gespecialiseerde toezichthouder die in alle fasen van bulkinterceptie toezicht houdt. Deze toezichthouder neemt in de ex ante fase bindende beslissingen en kan aanbevelingen doen aan de verantwoordelijke minister voor de dienst, en houdt in de ex durante- en ex post-fase toezicht. Opvallend is dat in het Verenigd Koninkrijk het nationaal cybersecuritycentrum onderdeel is van de GHCQ. De IPCO houdt ook op deze organisatie toezicht, maar publiceert daar geen afzonderlijke rapporten over, zoals wel het geval is in bijvoorbeeld Denemarken. De IPCO presenteert haar onderzoeksresultaten voornamelijk via een uitgebreid jaarverslag.

Een kenmerkend aspect van de IPCO is de – naar eigen zeggen - 'symbiotische relatie' tussen haar afdelingen. De Judicial Commissioners controleren vooraf aanvragen voor de inzet van bevoegdheden, terwijl de inspecteurs achteraf toezicht houden door middel van inspecties. Deze afdelingen overleggen met elkaar, wat resulteert in een zekere wisselwerking. Tegelijkertijd moet de IPCO haar aandacht verdelen over meer dan 600 organisaties, waardoor het toezicht op bulkinterceptie slechts een relatief klein deel van haar werkzaamheden uitmaakt.

Het toezichtstelsel in het Verenigd Koninkrijk kenmerkt zich verder door de significante rol die is toegekend aan de IPT, een gespecialiseerde rechtbank die klachten van belanghebbenden behandelt. De IPT kan bindende beslissingen nemen, bijvoorbeeld door het bevelen tot vernietiging van onrechtmatig verwerkte gegevens of het toekennen van schadevergoedingen aan belanghebbenden. Het EHRM heeft deze rol van het IPT in jurisprudentie als 'robuust' omschreven en erkent dat het een effectief rechtsmiddel kan bieden aan betrokkenen.

# Hoofdstuk 7: Conclusie

Dit rapport beantwoordt de vraag hoe de toetsings- en toezichtsystemen op inlichtingen- en veiligheidsdiensten zijn ingericht in Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk. Voor het beantwoorden van deze onderzoeksvraag is de volgende aanpak gehanteerd. In hoofdstuk 2 is een normatief kader opgesteld, gebaseerd op EHRM-jurisprudentie over bulkinterceptie en de vereisten voor toezicht uit Conventie 108+. Dit kader diende als leidraad om te bepalen welke vereisten aan het toezicht kunnen worden gesteld bij de inzet van bulkinterceptie als bevoegdheid door inlichtingen- en veiligheidsdiensten. Vervolgens is voor elk van de genoemde landen nagegaan hoe zij zich tot deze toezichtsvereisten verhouden.

Het is duidelijk dat de jurisprudentie van het EHRM een significante invloed heeft gehad op de nationale toezichtsystemen in elk van de onderzochte landen. In Denemarken, Zweden en het Verenigd Koninkrijk heeft deze jurisprudentie geleid tot wetsvoorstellen waarbij het toezicht in alle fasen werd verstrekt. Voor Frankrijk betekende dit meer een bevestiging dat hun bestaande toezichtstelsel voldoet aan de vereisten van het EHRM. In Zweden werd, naast de invloed van het EHRM, in een evaluatie en wetsvoorstel veel aandacht besteed aan Conventie 108+, vanwege de specifieke toezichtseisen in het nationale veiligheidsdomein. Frankrijk is tot nu toe het enige land onderzocht dat Conventie 108+ heeft geratificeerd.

De analyse in hoofdstuk 2 toont aan dat effectief en onafhankelijk toezicht op de toepassing van bulkinterceptie door inlichtingen- en veiligheidsdiensten noodzakelijk is in alle fasen van het proces, dat wil zeggen: vooraf (*ex ante*), tijdens (*ex durante*), en achteraf (*ex post*). Het EHRM benadrukt het belang van een effectief rechtsmiddel (de ‘remedy’) in het ex post toezicht. Bij de beoordeling van een nationaal toezichtstelsel hanteert het EHRM een 'holistische benadering', waarbij vereist is dat toezichthouders onafhankelijk en effectief zijn. De focus ligt daarbij niet zozeer op de individuele toezichtmechanismen, maar op de doeltreffendheid van het stelsel als geheel. Conventie 108+ identificeert factoren die de onafhankelijkheid en effectiviteit van een toezichthouder waarborgen, zoals de benoemingsprocedure en samenstelling van de toezichthoudende autoriteit, de beschikbare infrastructuur (inclusief financiële, technische en personele middelen), de bevoegdheid om zelfstandig gegevens te verzamelen en personeel aan te stellen, de mogelijkheid tot het raadplegen van deskundigen en externe consultaties, en het vermogen om beslissingen te nemen zonder onderhevig te zijn aan externe inmenging.

Uit de literatuur, jurisprudentie-analyse en Conventie 108+ blijkt dat verschillende instanties een toezichtsrol kunnen vervullen in elke fase van het toezicht. Tot de 'formele toezichthouders' behoren rechterlijke instanties en specialistische toezichthouders. Andere instanties, met uiteenlopende functies, spelen ook een rol op verschillende aspecten van het toezicht op inlichtingen- en veiligheidsdiensten. Deze instanties zijn in hoofdstuk 2 gecategoriseerd als 'overige instanties'. Daaronder vallen bijvoorbeeld nationale rekenkamers, parlementaire onderzoekscommissies en ombudsman-instanties. Voor zover relevant zijn deze instanties per land kort omschreven.

Figuur 1 in hoofdstuk 2 illustreert de fasen van toezicht op bulkinterceptie en welke formele instanties daar een rol in kunnen spelen. In de hoofdstukken 3 tot en met 6 wordt de concrete invulling van het toezicht uiteengezet ten aanzien van bulkinterceptie in Denemarken, Zweden,

Frankrijk en het Verenigd Koninkrijk. In elk hoofdstuk is het toezichtstelsel per land gevisualiseerd aan de hand van het toezichtsmodel in Figuur 1.

*Algemene typering inlichtingen- en veiligheidsdiensten*

Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk delen met elkaar dat hun inlichtingen- en veiligheidsdiensten bulkinterceptie inzetten ter bescherming van de nationale veiligheid. Er is echter een grote diversiteit aan inlichtingen- en veiligheidsdiensten per land, evenals aanzienlijke verschillen in welke diensten onder toezicht staan van een specialistische toezichthouder. In Frankrijk en het Verenigd Koninkrijk vallen relatief veel inlichtingen- en veiligheidsdiensten, alsmede bijzondere opsporingsdiensten, onder het toezicht van één specialistische toezichthouder. Frankrijk heeft ongeveer twintig inlichtingen- en veiligheidsdiensten waar de specialistische toezichthouder verantwoordelijk voor is, terwijl de IPCO in het Verenigd Koninkrijk toezicht moet houden op meer dan 600 organisaties. Frankrijk is het enige land waar de toets vooraf op de inzet van vergaande bevoegdheden, het toezicht tijdens en achteraf, én de behandeling van klachten zijn ondergebracht bij één en dezelfde specialistische toezichthouder op de inlichtingen- en veiligheidsdiensten.

Het valt ook op dat elk van de landen een nationaal cybersecuritycentrum heeft, waarvan de meeste een sterke relatie onderhouden met de nationale SIGINT-organisatie (bijvoorbeeld door inbedding van het centrum binnen deze organisatie). Niet alle cybersecuritycentrums staan onder specialistisch toezicht. Deze centra zijn echter verantwoordelijk voor het tegengaan van cyberaanvallen die de nationale veiligheid bedreigen en mogen daartoe, in meer of mindere mate, internetverkeer monitoren. Denemarken is het enige land waar de specialistische toezichthouder op inlichtingen- en veiligheidsdiensten ook toezicht houdt op het nationaal cybersecuritycentrum en daarover elk jaar rapporteert. In het Verenigd Koninkrijk valt het nationale cybersecurity centrum (NCSC) onder de communicatie-inlichtingendienst, die op haar beurt onder toezicht staat van een gespecialiseerde toezichthouder.

*Verschillen in toezichtstelsels*

In elk land is er een specialistische toezichthouder die toeziet op de rechtmatigheid van de gegevensverwerkingen bij bulkinterceptie. Daar houden de overeenkomsten echter ongeveer mee op; op detailniveau verschilt de regeling van het toezicht per land aanzienlijk.

De verschillen in het toezicht in Denemarken, Zweden, Frankrijk en het Verenigd Koninkrijk worden hieronder per fase van toezicht gepresenteerd.

*Ex ante fase*

De meeste landen hebben een onafhankelijke instantie of rechter die toestemming moet geven voor de inzet van bulkinterceptie, zoals vereist in de ex ante fase door het EHRM.

In Zweden voert een specialistische rechtbank een rechtmatigheidstoets uit op aanvragen voor bulkinterceptie. Kenmerkend is dat er in Zweden ook een speciaal aangestelde ‘privacyfunctionaris’ betrokken is bij dit oordeel, om de privacybelangen van betrokkenen te beschermen. Een wetsvoorstel uit 2025 voorziet in een uitbreiding van de taken van dit ‘Defensie Inlichtingenhof’ met betrekking tot bulkdatasets (ook afkomstig uit andere bronnen dan bulkinterceptie) en in een rol als beroepsinstantie voor beslissingen over gegevensverwerking door toezichtsinstanties.

In Frankrijk en het Verenigd Koninkrijk voeren de specialistische toezichthouders deze rechtmatigheidstoets op de aanvragen uit. In het Verenigd Koninkrijk is dit oordeel in eerste en laatste instantie bindend, terwijl in Frankrijk een beroepsprocedure bij de Conseil d'État bestaat als de CNCTR de aanvraag niet rechtmatig acht.

In Denemarken ontbreekt momenteel een voorafgaande toets door een onafhankelijke instantie of rechter. De Deense regering tracht in een wetsvoorstel uit 2025 alsnog een voorafgaande toets door een speciale rechtbank te regelen.

*Ex durante fase*

In elk van de onderzochte landen is een specialistische toezichthouder aanwezig die de rechtmatigheid van gegevensverwerkingen controleert. Deze vorm van toezicht vindt ook ex durante plaats.

De toezichthouders in Denemarken, Frankrijk en het Verenigd Koninkrijk beschrijven in detail hoe zij deze ex durante controle uitvoeren, met name door middel van geautomatiseerde controlesystemen en de controle van logging via inspecties. In Frankrijk is zelfs een speciale organisatie opgericht om de specialistische toezichthouder CNCTR te faciliteren bij de toegang tot en 'online controles' van de systemen van de Franse inlichtingen- en veiligheidsdiensten.

In Zweden wordt deze vorm van doorlopend toezicht niet expliciet genoemd in publieke stukken, zoals jaarverslagen. Een kenmerkend aspect van het Zweedse systeem is dat verschillende toezichthouders gelijktijdig toezicht houden op de inzet van bevoegdheden door de inlichtingen-, veiligheids- en opsporingsdiensten. Eén toezichthouder (Siun) houdt specifiek toezicht op de nationale SIGINT-organisatie, terwijl een andere toezichthouder (Sin) toezicht houdt op de politie-inlichtingendienst. De toezichthouder IMY, die zich richt op de bescherming van persoonsgegevens (ook ten aanzien van de nationale SIGINT-organisatie en de Zweedse krijgsmacht), heeft stevige (bindende) bevoegdheden, maar lijkt niet erg actief te zijn in het toezicht op bulkinterceptie en behandelt geen klachten van individuen. In een wetsvoorstel uit 2025 is voorgesteld deze taak bij de specialistische toezichthouder Siun onder te brengen.

*Ex post fase*

Elk van de onderzochte landen kent een specialistische toezichthouder voor het ex post toezicht op inlichtingen- en veiligheidsdiensten, inclusief hun bulkinterceptie-activiteiten. Deze toezichthouders publiceren hun onderzoeksresultaten in een jaarrapport. Daarbij valt op dat niet elke specialistische toezichthouder bij het constateren van onrechtmatigheden bindende beslissingen kan nemen. Naar aanleiding van de uitspraak *Centrum för Rättvisa e.a.* zijn er veel ontwikkelingen op wetgevingsgebied om verzoekers een effectief rechtsmiddel te bieden via een klachtregeling. De invulling daarvan – via een afdeling bij de specialistische toezichthouder of een speciale rechtbank – verschilt per land. In *Association Contrafraternelle de la Presse Judiciaire e.a.* heeft het EHRM bevestigd dat het Franse model ook de EVRM-toets doorstaat.

Volgens het EHRM is de toegang tot een effectief rechtsmiddel in Frankrijk en het Verenigd Koninkrijk 'robuust'. In deze landen worden klachten van vermeend onrechtmatig handelen door de diensten behandeld in een rechtszaak door een specialistische rechtsinstantie (VK) of in beroep door een gespecialiseerde kamer van de hoogste bestuursrechter (Frankrijk). Het

EHRM vindt het daarbij belangrijk dat een eerlijke en, voor zover mogelijk, adversaire procedure plaatsvindt. De Franse bestuursrechter en de Britse specialistische rechtsinstantie hebben ook toegang tot staatsgeheime informatie en kunnen documenten bij de inlichtingen- en veiligheidsdiensten opvragen. Ten slotte kunnen deze instanties bindende beslissingen nemen, zoals het bevelen van de vernietiging van onrechtmatig verwerkte gegevens en het toekennen van een schadevergoeding aan de betrokkenen.

De ex post toezichtsfase in Denemarken kent aanzienlijke beperkingen. Deense wet- en regelgeving bevat geen gedetailleerde regeling voor bulkinterceptie, en de specialistische toezichthouder TET heeft geen toegang tot de ruwe gegevens die met SIGINT worden verzameld. Bovendien is de huidige taakstelling van TET beperkt door de focus op de rechtmatigheid van gegevensverwerkingen. De verantwoordelijke minister van een inlichtingen- en veiligheidsdienst (FE) heeft het laatste woord over wetsinterpretaties, wat vragen oproept over onafhankelijkheid. Ten slotte valt op dat het toezicht vaak beperkt is tot particulieren en rechtspersonen die in Denemarken verblijven. Een wetsvoorstel uit 2025 moet daar verandering in brengen. De specialistische toezichthouder TET zou daarbij een breder toezichtmandaat krijgen en de toezichthouder wordt in het voorstel versterkt met een 'College van toezicht op de inzagerechten', met bindende bevoegdheden waartegen geen beroep kan worden aangetekend bij een rechter.

In 2025 is in Zweden naar aanleiding van de uitspraak *Centrum för Rättvisa e.a. t. Zweden* wet- en regelgeving aangepast, waardoor een nieuw besluitvormingsorgaan is ingesteld binnen de specialistische toezichthouder Siun voor de klachtbehandeling. Denemarken en Zweden kozen voor de instelling van een aparte kamer binnen een specialistisch toezichthouder, met andere commissieleden dan de commissieleden die voor de afdeling toezicht beslissingen nemen. De achtergrond van deze keuze is gelegen in veiligheidsredenen (de omgang met staatsgeheime informatie), de specialistische kennis van de medewerkers en commissieleden van deze toezichthouders, en efficiëntie (het delen van een secretariaat en infrastructuur).

*Aanbevolen vervolgonderzoek*

De mogelijkheden voor toekomstig onderzoek zijn deels gelegen in de beperkingen van dit rapport. Hieronder worden drie richtingen voor vervolgonderzoek toegelicht.

In dit rapport zijn de vereisten voor toezicht op inlichtingen- en veiligheidsdiensten geïdentificeerd in de context van de inzet van bulkinterceptie. Niet voor elke bevoegdheid is een voorafgaande toets door een onafhankelijke of rechterlijke instantie vereist. Het verschilt daarom ook per land in hoeverre een onafhankelijke voorafgaande toets ook een rol speelt bij de inzet van andere bevoegdheden en bij andere instanties, zoals opsporingsinstanties. Vervolgonderzoek zou zich meer kunnen richten op het toezicht op andere bevoegdheden, het toezichtstelsel in andere landen, en het toezicht op andere overheidsinstanties die zich bezighouden met opsporing of het verzamelen van inlichtingen in andere domeinen, zoals het opsporings- of het fiscale inlichtingendomein.

Uit dit onderzoek komt ook naar voren dat de positie en het toezicht op nationale cybersecuritycentrums nog sterk in beweging zijn. Gezien de grootschalige gegevensverwerkingen die in deze centrums plaatsvinden, kan het interessant zijn de noodzaak tot regelgeving en toezicht nader te onderzoeken. Verder kan door middel van empirisch

onderzoek, of vanuit een andere discipline, meer onderzoek worden gedaan naar het daadwerkelijke functioneren van de toezichthouders op inlichtingen- en veiligheidsdiensten.

Tot slot richtte dit onderzoek zich op de nationale dimensie van het toezicht op inlichtingen- en veiligheidsdiensten. Duidelijk is dat inlichtingen- en veiligheidsdiensten ook samenwerken, bijvoorbeeld via gezamenlijke operaties, gegevensuitwisseling of gezamenlijke gegevensverwerkingen. Dit alles vindt plaats terwijl het toezicht nationaal is geregeld. Het samenwerkingsverband van toezichthouders, de 'Intelligene Oversight Working Group', signaleert daarom ook een "toezichtsgat" op deze gezamenlijke activiteiten. Dat geeft aanleiding tot nader onderzoek naar de noodzaak tot toezicht op gezamenlijke inlichtingenoperaties.

# Geraadpleegde literatuur

*Boeken*


Braithwaite 2006
J. Braithwaite, 'Accountability and Responsibility Through Restorative Justice' in: M. Dowdle (red.) *Rethinking Public Accountability*, Cambridge: Cambridge University Press 2006, p. 33-51.

Born & Wills 2012
H. Born & A. Wills (red.), *Overseeing Intelligence Services. A Toolkit*, Geneve: DCAF (met financiering van het ministerie van Buitenlandse Zaken) 2012.

Forcese 2012
C. Forcese, 'Handling Complaints about Intelligence Services', in: H. Born & A. Wills 2012, p. 181-193.

Wills 2012
Wills, 'Financial Oversight of Intelligence Services', in: H. Born & A. Wills 2012, p. 151-178.

De Terwange 2022
C. De Terwangne, 'Privacy and data protection in Europe', in: G. González, R. Van Brakel & P. De Hert (red.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, Cheltenham: Edward Elgar Publishing 2022, p. 10-35.

Gaskarth 2020
J. Gaskarth, *Secrets and spies: U.K. intelligence accountability after Iraq and Snowden (Insights: critical thinking on international affairs)*, Washington, D.C.: London: Brookings Institution Press, Chatham House 2020.

Hartvigsen, Hartmann & Diderichsen 2024
M. Hartvigsen, M. Hartmann, A. Diderichsen, 'Intelligence Oversight as an Institutional Battlefield. The Danish Experience', in: K. Vrist Rønn, A. Diderichsen, M. Hartmann, M. Hartvigsen (red.), *Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism?*, Londen: Routledge, Taylor & Francis Ltd 2024.

Jalalzai 2016
M.K. Jalalzai, *Fixing the EU intelligence crisis: intelligence sharing, law enforcement and the threat of chemical biological and nuclear terrorism*, New York: Algora Publishing 2016.

Leigh 2019
I. Leigh, 'Intelligence Law and Oversight in the UK', in: J.-H. Dietrich & S. Sule (eds.), *Intelligence Law and Policies in Europe: A Handbook*, Oxford: Hart Publishing 2019.

Ördén 2025
H. Ördén, ‘Trust Games in Denmark and Sweden: Unpacking Trust in International Intelligence Cooperation on SIGINT’, in: K. Vrist Rønn, A. Diderichsen, M. Hartmann, M. Hartvigsen (red.), *Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism?*, Londen: Routledge, Taylor & Francis Ltd 2024.

Partington 2021
M. Partington, *Introduction to the English legal system*, Oxford: Oxford University Press 2021.

Weaver 2024
J.M. Weaver, ‘United Kingdom’, in: J.M. Weaver, *National Security Through the Lens of the ‘Five Eyes’ Nations*, Cham: Springer Nature Switzerland 2024, p. 87-104.

*Artikelen*

Andersen e.a. 2022
S.J. Andersen, M.E. Hansen, P.H.J. Davies, ‘Oversight and Governance of the Danish Intelligence Community’. *Intelligence and National Security* 2022/37 (2), p. 241-261.

Bochel & Defty 2017
H. Bochel & A. Defty, ‘Parliamentary Oversight of Intelligence Agencies: Lessons from Westminster’, in: *Open Reports Series*, Cambridge, UK: Open Book Publishers 2017, p. 103-124.

Bovens & Wille 2021
M. Bovens & A. Wille, ‘Indexing watchdog accountability powers a framework for assessing the accountability capacity of independent oversight institutions’, *Regulation & Governance* 2021/15, p. 856–876.

Constantino & Wagner 2024
J. Constantino & B. Wagner, ‘Accountability and oversight in the Dutch intelligence and security domains in the digital age’, *Frontiers Political Science* 2024/6, p. 1-21.

De Graaff & Hijzen 2018
B.G.J. De Graaff & C. Hijzen, ‘Zwijgen is zilver en spreken is goud’, *Justitiële verkenningen* 2018/44(1), p. 148-157.

Hagens & Ryngaert 2018
M. Hagens & C.M.J. Ryngaert, ‘Massasurveillance en privacy: De betekenis van het EHRM-arrest Big Brother Watch e.a. t. het Verenigd Koninkrijk voor het EU-recht’, *Tijdschrift voor Internetrecht* 2018 nr. 5/6, p. 209-217.

Hansén 2023
D. Hansén, ‘Assessing intelligence oversight: the case of Sweden’, *Intelligence and National Security* 2023/38(6), p. 938–955.

Jansen 2022
R.H.T. Jansen, ‘Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten’, *Computerrecht* 2022/51(2), p. 97-109.

Jansen 2025
R.H.T. Jansen, ‘Kabelinterceptie door de AIVD en de MIVD’, *NJB* 2025/697, p. 1-16.

Jansen & Reijneveld 2021
R.H.T. Jansen & M.D. Reijneveld, ‘Conventie 108+ en (toezicht op) gegevensverwerkingen in het nationale veiligheidsdomein’, *Computerrecht* 2021/208, p. 411-422.

Jansen & Reijneveld 2022
R.H.T. Jansen & M.D. Reijneveld, ‘Council of Europe · Convention 108+, the GDPR, and Data Processing in the National Security Domain’, *European Data Protection Law Review* 2022/8(3), p. 423-430.

Klamberg 2009
M. Klamberg, ‘FRA:s signalspaning ur ett rättsligt perspektiv’, *Svensk Juristtidning* 2009/4, p. 519-541.

Klein 2023
A. Klein, ‘Safe and Free: National-Security Surveillance and Safeguards Across Rule-of-Law States’, *Lawfare,* lawfaremedia.org, 15 december 2023.

Koch 2023
P.G. Koch, ‘Retsgrundlag for efterretningstjenester i en ny tid’, *Juristen* 2023, nr.1, p. 11-19.

Oerlemans & Hagens 2019
J.J. Oerlemans & M. Hagens, ‘Privacy en bulkinterceptie in de Wiv 2017’, *Ars Aequi* 2019/7, p. 560-568.

Ukrow 2018
J. Ukrow, ‘Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108’*, European Data Protection Law Review* 2018/2, p. 239-247.

Van Puyvelde 2013
D.V. van Puyvelde, ‘Intelligence accountability and the role of public interest groups in the United States’, *Intelligence and National Security* 2013/28(2), p. 139–158.

*Rapporten*

Anderson 2015
D.W.K. Anderson, *A question of trust: report of the Investigatory Powers review*, London: The Stationery Office 2015.

Anderson 2016
D.W.K. Anderson, *Report of the Bulk Powers Revie*w, London: Dandy Booksellers Ltd 2016.

Anderson 2023
D.W.K. Anderson, 'Independent Review of the Investigatory Powers Act 2016', *SSRN Electronic Journal 2023*, p. 1-125.

CTIVD 2022
Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, *Jaarverslag 2022*, Den Haag 2022, ctivd.nl, 20 april 2023.

CFCS 2023
Danish Intelligence Oversight Board, *Annual report 2023*, Danish Centre for Cyber Security (CFCS), mei 2024.

Chancellor's speech to GCHQ 2015
G. Osborne, *Chancellor's speech to GCHQ on cyber security*, gov.uk, 17 november 2015.

DCAF 2017
Geneva Centre for Security Sector Governance (DCAF), *Intelligence Oversight. Ensuring accountable intelligence within a framework of democratic governance*, dcaf.ch, 1 september 2017.

Europees Parlement 2011
H. Born, M. Scheinin & M. Wiebush, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (study), Directorate-General for International Policies, European Parliament, Brussel 2011.

Evaluatiecommissie Wiv 2017
Evaluatiecommissie Wiv 2017 (Commissie Jones-Bos), *Evaluatie 2020 Wet op de inlichtingen- en veiligheidsdiensten 2017*, bijlage bij *Kamerstukken II* 2020/21, 34588 nr. 88, 2021, p. 1-180.

Dawson & Godec 2017
J. Dawson & S. Godec, *Oversight of the intelligence agencies: a comparison of the 'Five Eyes' nations* (briefing paper), House of Commons 2017.

Handbook on European data protection law 2018
EU Agency for Fundamental Rights and Council of Europe*, Handbook on European data protection law*, fra.europa.eu, 2018.

Hannigan 2019
R. Hannigan, *Organising a Government for Cyber. The Creation of the UK's National Cyber Security Centre* (Occasional paper), Royal United Service Institute for Defence and Security Studies 2019, rusi.org.

Intelligence and Security Committee 2015
Intelligence and Security Committee, *Privacy and security: a modern and transparent legal framework*, London: House of Commons Intelligence and Security Committee 2015, isc.independent.co.uk.

IPCO Jaarrapport 2017
Investigatory Powers Commissioner's Office, *Annual Report 2017*, ipco.org.uk, 31 januari 2019.

IPCO Jaarrapport 2020
Investigatory Powers Commissioner's Office, *Annual Report 2020*, ipco.org.uk, 6 januari 2022.

IPCO Jaarrapport 2021
Investigatory Powers Commissioner's Office, *Annual Report 2021*, ipco.org.uk, 20 maart 2023.

IPCO Jaarrapport 2022
Investigatory Powers Commissioner's Office, *Annual Report 2022*, ipco.org.uk, 26 maart 2024.

IPT Report 2016-2021
Investigatory Powers Tribunal, *Report 2016-2021*, ipt-uk.com/investigatorypowerstribunal.org.uk, 2022.

Jaarverslag FE 2023
Danish Intelligence Oversight Board, *Annual report 2023*, Danish Defence Intelligence Service (DDIS), mei 2024.

FRA 2017
EU Agency for Fundamental Rights (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, Luxembourgh: Publications Office of the European Union 2017.

FRA 2018
EU Agency for Fundamental Rights (FRA) and Council of Europe*, Handbook on European data protection law*, Luxemburg: Publications Office of the European Union 2018, fra.europa.eu.

FRA 2023
European Agency for Fundamental Rights (FRA), *Surveillance by Intelligence Services. Fundamental Rights Safeguards and Remedies in the EU – 2023 update*, fra.europa.eu.

Leigh 2023
I. Leigh, *National Security Surveillance in the United Kingdom* (Country Study), Strauss Center for International Security and Law 2023, p. 1-19, safeandfree.io.

*National Intelligence Machinery* 2010
Cabinet Office & National Security and Intelligence, *National Intelligence Machinery, Cabinet Office and National security and intelligence* 2010, p. 38, gov.uk.

SOU 2023
Statens Offentliga Utredningar (SOU), *Tussentijds verslag van de commissie inzake de herziening van de wet op de signaalinlichtingenactiviteiten op defensiegebied,* Stockholm: Elanders Sverige AB 2023 (*Signalspaning i försvars-underrättelseverksamhet - frågor med anledning av Europadomstolens dom. Delbetänkande av Utredningen om Översyn av lagen om signalspaning i försvarsunderrättelseverksamhet* 2023).

SOU 2025
Statens Offentliga Utredningar (SOU), *Verwerking van persoonsgegevens door de Veiligheidspolitie. Verslag van het onderzoek naar de verwerking van persoonsgegevens door de Veiligheidsdienst*, Stockholm: Elanders Sverige AB 2025 (*Säkerhetspolisens behandling av personuppgifter. Beänkande av Utredningen om Säkerhetspolisens informationshantering* 2025)

TET jaarverslag 2022
Danish Intelligence Oversight Board (TET), *Annual report 2022*, tet.dk, juni 2023.

TET jaarverslag 2023
Danish Intelligence Oversight Board (TET), *Annual report 2023*, tet.dk, mei 2024.

Venice Commission 2007
European Commission for Democracy Trough Law (Venice Commission), *Report on the Democratic Oversight of the Security Services* (aangenomen tijdens de 71e plenaire vergadering op 1-2 juni 2007), studienr. 388/2006, venice.coe.int.

Wallin 2018
Fredrik Wallin, *A Brief History of the FRA. From Morse to Cyber Defence*, FRA 2018, fra.se.

Wetzling & Dietrich 2021
Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (geschreven door T. Wetzling & C. Dietrich), *Report on the need for a Guidance note on Article 11 of the modernised Convention 108* (11 juni 2021), Straatsburg: Directoraat Generaal Mensenrechten en Rechtstaat 2021.

Weltzling & Vieth 2018
T. Wetzling & K. Vieth, *Upping the ante on bulk surveillance an international compendium of good legal safeguards and overzicht innovations* (Publication Series on Democracy, vol. 50), Heinrich Böll Stichting 2018.

## Jurisprudentie

EHRM 6 september 1978, nr. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a. t. Duitsland*)

EHRM 24 april 1990, nr. 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584 (*Huvig t. Frankrijk*)

EHRM 24 april 1990, nr. 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin t. Frankrijk*)

EHRM 29 juni 2006, nr. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, *EHRC* 2007/13, m.nt. Loof (*Weber en Saravia t. Duitsland)*

EHRM 1 juli 2008, nr. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300, *EHRC* 2008/100, m.nt. Van der Velde (*Liberty e.a. t. het Verenigd Koninkrijk*)

EHRM 18 mei 2010, nr. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905 (*Kennedy t. Verenigd Koninkrijk*)

EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, *NJ* 2017/185, m.nt. Dommering, *EHRC* 2016/87, m.nt. Hagens (*Roman Zakharov t. Rusland*)

EHRM 13 september 2018, nr. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, *Computerrecht* 2018/252, m.nt. J.J. Oerlemans, *EHRC* 2018/208, m.nt. M. Hagens (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*)

EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, *EHRC Updates* 2021, m.nt. M. Hagens & J.J. Oerlemans (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*)

EHRM 25 mei 2021, nr. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, *EHRC Updates* 2021, m.nt. M. Hagens & J.J. Oerlemans; *JBP* 2021/62, m.nt. E. Moyakine; *NJ* 2021/361, m nt. E.J. Dommering, *NJB* 2021/1804, m. nt. M.M. Groothuis (*Centrum för Rättvisa t. Zweden*)

EHRM 10 december 2024, nrs. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15, 59621/15, 30635/17, 30636/17, ECLI:CE:ECHR:2024:1210DEC004952615 (*Association Confraternelle de la Presse Judiciare e.a. t. Frankrijk*)