Raad van de Europese Unie

Brussel, 13 maart 2025
(OR. en)

15941/2/24
REV 2

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

NOTA

van:	het voorzitterschap
aan:	de delegaties
nr. vorig doc.:	11281/24
Betreft:	Concluding report of the High-Level Group on access to data for effective law enforcement

Het voorzitterschap verstrekt de delegaties in de bijlage namens de beide voorzitters van de Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving (GHN) het eindverslag van de GHN.

Deze herziene versie weerspiegelt redactionele wijzigingen die tijdens de taalkundige toetsing zijn aangebracht.

BIJLAGE

Eindverslag van de Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving

15 november 2024

De onderstaande standpunten zijn uitsluitend die van de groep op hoog niveau en mogen niet worden beschouwd als representatief voor het officiële standpunt van de Europese Commissie of de Raad.

De aanbevelingen van de Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving moeten worden uitgevoerd met volledige inachtneming van de bevoegdheden van de lidstaten. Zij hebben alleen betrekking op rechtshandhavingsactiviteiten en commerciële instrumenten die voor gerechtelijke doeleinden worden gebruikt en laten de exclusieve verantwoordelijkheid van de lidstaten voor hun nationale veiligheid onverlet. De aanbevelingen hebben derhalve geen betrekking op soevereine instrumenten en instrumenten die uitsluitend voor nationale veiligheidsdoeleinden worden gebruikt en/of zijn ontwikkeld.

Inhoud

Samenvatting

De Europese Unie is een ruimte van vrijheid, veiligheid en recht, waarin de grondrechten en de verschillende rechtsstelsels en -tradities van de lidstaten worden geëerbiedigd. Zij tracht een hoge mate van veiligheid[1] te waarborgen door middel van maatregelen ter voorkoming en bestrijding van criminaliteit en ter vergemakkelijking van de coördinatie en samenwerking tussen rechtshandhavings- en rechterlijke instanties en andere bevoegde autoriteiten.

Technologische ontwikkelingen en de digitalisering van onze samenlevingen hebben geleid tot aanzienlijke veranderingen in het dagelijks leven van burgers en tot nieuwe uitdagingen voor rechtshandhavings- en rechterlijke instanties bij het waarborgen van een hoge mate van veiligheid, zowel op nationaal als op EU-niveau. In het huidige digitale tijdperk bevat bijna elk strafrechtelijk onderzoek een digitale component. Dit werd in april 2023 aan de orde gesteld in het verkennend document voor de Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving:

> Technologieën en instrumenten […] worden ook misbruikt voor criminele doeleinden. Door deze ontwikkeling wordt het steeds moeilijker om in de hele EU te zorgen voor doeltreffende rechtshandhaving, de openbare veiligheid te waarborgen, criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen, en tegemoet te komen aan de legitieme verwachtingen van slachtoffers met betrekking tot gerechtigdheid en schadevergoeding. Als dit probleem niet wordt aangepakt, bestaat er een reëel risico dat criminelen door deze ontwikkeling "onder de radar" kunnen opereren […]. Dit vormt een serieuze dreiging voor de veiligheid van het individu en de samenleving, en kan uiteindelijk een belemmering vormen voor de positieve verplichting van de staat om de rechtstaat en de democratische samenleving te waarborgen[2].

[1] In dit document wordt onder "veiligheid" de bestrijding van criminaliteit of de voorkoming van bedreigingen van de openbare veiligheid verstaan.

[2] Doc. 8281/23 van 13 april 2023.

Het recht van eenieder op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie, en het recht op bescherming van persoonsgegevens worden gewaarborgd door het Handvest van de grondrechten van de EU. De vertrouwelijkheid van communicatie, zowel in geschrifte als telefonisch, is een belangrijke verworvenheid van democratische samenlevingen en een waarborg dat noch de staat, noch particuliere actoren inbreuk kunnen maken op de vrijheid van meningsuiting van personen, en heeft de totstandkoming van een florerend maatschappelijk middenveld mogelijk gemaakt. Het genot van die rechten kan onderworpen zijn aan wettelijke beperkingen, met name met betrekking tot maatregelen gericht op het waarborgen van de nationale veiligheid, defensie of de openbare veiligheid, of op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van elektronische-communicatiesystemen, mits deze maatregelen in een democratische samenleving noodzakelijk, redelijk en proportioneel zijn. Rechtshandhavings- en rechterlijke instanties kunnen daarom schriftelijke communicatie openen en lezen, telefoongesprekken onderscheppen en gesprekken afluisteren, indien dit noodzakelijk, proportioneel en gerechtvaardigd wordt geacht, dergelijke maatregelen in overeenstemming zijn met de toepasselijke wettelijke bepalingen, en bij de uitvoering ervan de grondrechten in acht worden genomen. Alle bevoegde autoriteiten zouden van deze mogelijkheid moeten kunnen gebruikmaken, ongeacht de technologische ontwikkelingen. Door de wildgroei aan nieuwe vormen van interpersoonlijke communicatie in de afgelopen jaren zal de gehele samenleving zich moeten aanpassen aan een nieuwe realiteit. Wij moeten ervoor zorgen dat de communicatie tussen burgers beschermd blijft en dat rechtshandhavings- en rechterlijke instanties tegelijkertijd hun plicht om burgers te beschermen, kunnen blijven vervullen door zware en georganiseerde criminaliteit en terrorisme te voorkomen en te bestrijden. Er moeten dringend aanpassingen worden doorgevoerd en de deskundigen verzoeken beleidsmakers snel op te treden, aangezien rechtshandhavingsinstanties nu al achterlopen op de technologische ontwikkelingen, wat directe gevolgen heeft voor hun vermogen om de rechten van burgers te beschermen.

Tijdens de informele bijeenkomst van de ministers van Justitie en Binnenlandse Zaken van 26 januari 2023 hebben de ministers van Binnenlandse Zaken de uitdagingen besproken die de technologische ontwikkelingen met zich meebrengen voor rechtshandhaving in het digitale tijdperk. Zij hebben ook hun bezorgdheid geuit over het feit dat door de toepasselijke regels en de uitlegging ervan in de jurisprudentie, in combinatie met praktische en operationele belemmeringen, rechtshandhavingsinstanties steeds meer moeilijkheden ondervinden bij de uitvoering van hun werkzaamheden, met name met betrekking tot het bewaren van en de toegang tot gegevens die nodig zijn om strafbare feiten te onderzoeken en te vervolgen[3].

[3] Zie doc. 7184/1/23 REV 1 van 23 maart 2023 voor een overzicht van de opmerkingen van de lidstaten.

De Raad heeft naar aanleiding van deze bespreking zijn goedkeuring gehecht aan de oprichting van een **groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving (GHN)**[4] voor de ontwikkeling van een strategische, toekomstgerichte visie op doeltreffende en rechtmatige toegang tot gegevens, elektronisch bewijs en informatie in het digitale tijdperk voor rechterlijke en rechtshandhavingsinstanties.

De GHN had tot doel oplossingen te vinden voor het probleem dat inherent verbonden is aan het toestaan van rechtmatige toegang tot gegevens, teneinde een hoge mate van veiligheid voor alle inwoners van de EU te waarborgen zonder afbreuk te doen aan de grondrechten, waaronder het recht op privacy en gegevensbescherming, en een hoog niveau van cyberbeveiliging te waarborgen, door middel van efficiënte en toekomstbestendige oplossingen.

De **42 aanbevelingen**[5] zijn het belangrijkste resultaat van de werkzaamheden van de GHN en komen op een moment dat er steeds meer wordt opgeroepen tot verantwoordingsplicht op het internet. De aanbevelingen hebben betrekking op de huidige en verwachte uitdagingen in verband met de technologische ontwikkelingen en moeten een alomvattende EU-aanpak mogelijk maken met het oog op doeltreffende strafrechtelijke onderzoeken en vervolgingen. De aanbevelingen zijn onderverdeeld in drie blokken: **capaciteitsopbouw, samenwerking met het bedrijfsleven en normalisatie, en wetgevingsmaatregelen.** In de aanbevelingen wordt gewezen op de problemen die rechtshandhavingsinstanties ervaren bij de toegang tot gegevens in een leesbaar formaat voor strafrechtelijke onderzoeken als gevolg van het gebrek aan geharmoniseerde verplichtingen inzake gegevensbewaring en strenge eisen op grond van de EU-jurisprudentie, het toenemende gebruik van eind-tot-eindencryptie en het gebrek aan medewerking van bepaalde niet-traditionele telecommunicatiediensten. Hoewel de GHN ingenomen is met de regels inzake elektronisch bewijs, wordt in de aanbevelingen gewezen op de beperkingen ervan bij het aanpakken van de aan encryptie gerelateerde problemen en opgeroepen tot nauwere samenwerking tussen rechtshandhavings- en rechterlijke instanties en dienstverleners om een permanente dialoog en wederzijds begrip omtrent operationele, technische en zakelijke behoeften te bevorderen en problemen bij de toegang tot geëncrypteerde gegevens op te lossen. Volgens deskundigen zal nauwere samenwerking tussen rechtshandhavingsinstanties en dienstverleners de situatie tot op zekere hoogte verbeteren, maar moeten voor een toekomstbestendige oplossing ook de verplichtingen voor dienstverleners om samen te werken wettelijk worden vastgelegd, zonder dat dit op algemene of systematische wijze afbreuk doet aan de encryptie voor gebruikers van een dienst.

---

4 Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving - Europese Commissie (europa.eu).

5 Aanbevelingen van de Groep op hoog niveau.

Op 13 juni 2024 **werd er in de Raad een gedachtewisseling gehouden** over de aanbevelingen van de GHN. De Raad was over het algemeen ingenomen met de werkzaamheden van de GHN-deskundigen en benadrukte dat er vaart moet worden gezet achter de werkzaamheden in verband met de toegang tot gegevens voor doeltreffende rechtshandhaving.[6] De ministers van Binnenlandse Zaken stelden de volgende prioriteiten vast: 1) vaststelling van een geharmoniseerd wetgevingskader van de EU inzake gegevensbewaring voor rechtshandhavingsdoeleinden; 2) vaststelling van regels voor doeltreffende toegang tot gegevens afkomstig van interpersoonlijke elektronische communicatie, en 3) vaststelling van juridische en technisch verantwoorde oplossingen om in individuele gevallen en op voorwaarde van een gerechtelijk bevel toegang tot geëncrypteerde gegevens te verkrijgen met het oog op het voorkomen, onderzoeken en vervolgen van zware en georganiseerde criminaliteit en terrorisme.

Voorts pleitten de ministers voor een grotere rol van de EU bij de normalisatie van protocollen en technologieën en voor een gecoördineerde aanpak van de certificering van digitale forensische instrumenten en procedures. Tot slot drongen zij aan op de ontwikkeling van een routekaart voor de uitvoering van de aanbevelingen, met een summier tijdschema, een beoordeling van de haalbaarheid en toereikende financiële middelen. Ook werd gewezen op het belang van coördinatie bij de uitvoering van de afzonderlijke aanbevelingen.

Dit eindverslag heeft tot doel een gedetailleerde beschrijving te geven van de uitdagingen die door de deskundigen zijn vastgesteld en verschillende mogelijkheden te presenteren voor de verdere werkzaamheden en de **operationalisering van de aanbevelingen**. Het bevat een overzicht van een aantal belangrijke kwesties die door de deskundigen zijn vastgesteld en die overeenkomstig het mandaat van de GHN als leidraad hebben gediend voor drie werkstromen.

Ten eerste is toegang tot gegevens van cruciaal belang voor **digitaal forensisch onderzoek**, zodat rechtshandhavingsinstanties in staat zijn bewijsmateriaal van elektronische apparaten te verzamelen en te analyseren. Deze gegevens bieden betrouwbare informatie over criminele activiteiten en helpen bij de identificatie van de verantwoordelijken voor strafbare feiten. Door de snelle ontwikkeling en het wijdverbreide gebruik van bepaalde technologieën, zoals encryptie, moeten rechtshandhavingsinstanties meer middelen inzetten voor de toegang tot geëncrypteerde gegevens en hun vaardigheden en technische oplossingen op dit gebied verbeteren. Doeltreffende grensoverschrijdende samenwerking, waarbij expertise wordt uitgewisseld, standaardinstrumenten en -procedures worden ontwikkeld en middelen worden gebundeld, kan in dit verband, ook met betrekking tot het gebruik van commerciële oplossingen, steun bieden. De deskundigen waren het er echter over eens dat capaciteitsopbouw alleen niet genoeg zal zijn om de rechtshandhavingscapaciteit te verbeteren. Sommige deskundigen beschouwden het verschaffen van toegang tot gegevens in een leesbaar formaat in duidelijk gereguleerde gevallen als een duurzamere langetermijnoplossing.

[6] Doc. 11281/24 van 21 juni 2024.

Ten tweede hebben rechtshandhavingsinstanties voor het doeltreffend onderzoeken en vervolgen van strafbare feiten geharmoniseerde en consistente wetgeving inzake **gegevensbewaring** nodig die volledig in overeenstemming is met de grondrechten. Door de snelle ontwikkeling van technologieën wordt de tijdige toegang van rechtshandhavingsinstanties tot relevante gegevens die door aanbieders worden opgeslagen, steeds waardevoller. Vooral de toegang tot door dienstverleners opgeslagen communicatiemetagegevens is van essentieel belang om verdachten te identificeren en inzicht te krijgen in hun activiteiten. Ook is aangetoond dat dit belangrijk is om vooruitgang in onderzoeken te boeken.

Ten derde is **legale interceptie** van essentieel belang voor het doeltreffend onderzoeken en vervolgen van georganiseerde criminaliteit en terroristische groeperingen. Dit stelt de autoriteiten in staat om, op grond van rechterlijke bevelen en met volledige inachtneming van de grondrechten, van dienstverleners te eisen de inhoud van communicatie, die waardevolle inzichten in criminele activiteiten biedt, te verstrekken. Gezien de verschuiving van traditionele aanbieders van communicatie naar over-the-top (OTT)-diensten, zoals gedefinieerd in het Europees wetboek voor elektronische communicatie[7], en het feit dat criminelen in toenemende mate overstappen op platforms met eind-tot-eindencryptie[8], moet voor de rechtmatige en directe toegang tot communicatie worden vastgesteld in hoeverre er behoefte is aan duidelijke regels voor samenwerking tussen rechtshandhavingsinstanties en technologiebedrijven, alsook aan nauwere samenwerking op EU-niveau om grensoverschrijdende verzoeken te vergemakkelijken.

De aanbevelingen en de inhoud van dit eindverslag weerspiegelen **enkel de verwachtingen en wensen van de GHN-deskundigen**.

Met dit verslag **heeft de GHN haar werkzaamheden afgerond** en verzoekt zij de Commissie, de lidstaten, het Europees Parlement en alle belanghebbenden om bij de ontwikkeling van maatregelen die gericht zijn op het aanpakken van de toegang tot gegevens voor een doeltreffende rechtshandhaving, inspiratie te putten uit de aanbevelingen en het verslag. Deze maatregelen moeten gepaard gaan met een krachtig verhaal waaruit blijkt dat er dringend aanzienlijke actie moet worden ondernomen om doeltreffende rechtmatige toegang tot gegevens te waarborgen.
De deskundigen moedigen alle EU-instellingen en -organen aan hier onverwijld werk van te maken door concrete initiatieven uit te voeren in het kader van een speciale routekaart.

---

[7] Richtlijn (EU) 2018/1972 van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie breidt een deel van het rechtskader voor traditionele telecommunicatie uit tot bedrijven die internetdiensten aanbieden via een telecommunicatie-infrastructuur die zij niet in eigendom of beheer hebben, waaronder nummeronafhankelijke interpersoonlijke communicatiediensten (NI-ICS).

[8] Dreigingsevaluatie van de georganiseerde internetcriminaliteit (Internet Organised Crime Threat Assessment – IOCTA) door Europol, 2024.

Rechtmatige toegang: de grootste uitdagingen

De afgelopen jaren zijn wij op veel gebieden beter geworden in het bestrijden van criminaliteit en het veilig houden van de EU. Wij werken doeltreffender samen op het gebied van rechtshandhaving en justitie, er zijn nieuwe wetgeving en instrumenten ter bestrijding van zware en georganiseerde criminaliteit ingevoerd en onze gezamenlijke inspanningen ter bestrijding van migrantensmokkel, mensenhandel, illegale handel in vuurwapens en drugs, corruptie en andere ernstige strafbare feiten zijn versterkt.

De rechtshandhavingsinstanties worden echter dagelijks geconfronteerd met nieuwe uitdagingen om onze burgers veilig te houden, met name als gevolg van de digitalisering van onze samenleving.

Digitale technologieën veranderen ons leven — van de manier waarop wij communiceren tot hoe wij leven en werken — en de maatschappelijke aspecten van deze verschuiving zijn niet gering. Digitalisering kan oplossingen bieden voor heel wat uitdagingen waarmee Europa en Europeanen worden geconfronteerd, en biedt zeer veel kansen, onder meer om banen te scheppen, onderwijs te bevorderen, het concurrentievermogen en innovatie te stimuleren, klimaatverandering te bestrijden en de groene transitie te vergemakkelijken.

Digitalisering zorgt er echter ook voor dat criminelen de technologische vooruitgang kunnen benutten om zowel online als offline misdrijven te plegen. Geëncrypteerde apparaten en apps, nieuwe exploitanten van communicatiemiddelen, virtuele particuliere netwerken (VPN's) enz. moeten de privacy van rechtmatige gebruikers helpen beschermen. Voor criminelen vormen zij echter ook doeltreffende middelen om hun identiteit te verbergen, hun criminele producten en diensten op de markt aan te bieden, op illegitieme wijze betalingen te verrichten en hun activiteiten en communicatie te verbergen, waardoor opsporing, onderzoek en vervolging doeltreffend worden omzeild. Hoewel er instrumenten en diensten bestaan die doelbewust zijn ontworpen en voornamelijk worden gebruikt voor illegale activiteiten, zijn er aanwijzingen dat criminelen steeds vaker misbruik maken van maatregelen ter bescherming van de privacy die beschikbaar worden gesteld door rechtmatige elektronischecommunicatiediensten. ***Rechtshandhavingsinstanties lopen in dit opzicht vaak achter op criminelen, aangezien zij niet over het geschikte personeel en de juiste instrumenten en middelen beschikken om deze uitdaging doeltreffend het hoofd te bieden.*** Als gevolg van deze ontwikkelingen is de toegang tot gegevens voor rechtshandhavingsdoeleinden de afgelopen jaren een belangrijk probleem geworden bij strafrechtelijke onderzoeken en vervolgingen. Niettemin zijn er opmerkelijke successen geboekt: zo zijn de rechtshandhavingsinstanties erin geslaagd versleutelde communicatienetwerken van criminele aard, zoals EncroChat en SkyECC, te ontmantelen en blijven zij operaties zoals "Desert Light" uitvoeren, in het kader waarvan in november 2022 een "superkartel" van cocaïnehandelaars werd opgerold. Het decryptieplatform van Europol heeft de afgelopen jaren verschillende onderzoeken op hoog niveau ondersteund, wat heeft bijgedragen tot succesvolle rechtshandhavingsacties tegen terrorisme en zware en georganiseerde criminaliteit.

Achter deze succesverhalen schuilen echter veel vertraagde en mislukte onderzoeken; beroepsbeoefenaars melden immers dat zij voortdurend moeilijkheden ondervinden om tijdig aan operationele behoeften te voldoen.

Door de autoriteiten rechtmatige toegang te verlenen, kunnen zij criminele communicatie doelgericht monitoren en onderscheppen en handelingen van criminelen verstoren, waardoor het gebruik van technologie voor criminele doeleinden wordt bemoeilijkt. Zonder een solide rechtskader en toereikende middelen zullen de rechtshandhavingsinstanties echter met onoverkomelijke moeilijkheden blijven kampen, en bestaat het risico dat essentieel bewijs om verschillende redenen buiten bereik blijft.

- **Gegevens zijn niet altijd beschikbaar**, met name wanneer ze zijn gewist als gevolg van inconsistente en ontoereikende regels inzake gegevensbewaring voor rechtshandhavingsdoeleinden. Deze lacune vormt een ernstige belemmering voor het onderzoek naar zware en georganiseerde criminaliteit. In de enquête die in 2023 in het kader van het Sirius-project[9] werd gehouden, haalde bijna de helft van de geraadpleegde onderzoekers het ontbreken van een geharmoniseerde regeling voor gegevensbewaring aan als voornaamste belemmering. Zonder geharmoniseerde regels bestaat het risico dat cruciale gegevens ontoegankelijk blijven, hetgeen de inspanningen om criminaliteit doeltreffend te bestrijden, ondermijnt.

- **Gegevens kunnen niet worden opgevraagd**, met name wanneer de data-extractie uit een apparaat mislukt. Bij gebrek aan de nodige vaardigheden, passende instrumenten en voldoende samenwerking met en door fabrikanten van apparaten is digitaal forensisch onderzoek moeilijk, duur en tijdrovend, soms zelfs helemaal onmogelijk. Deze ernstige tekortkomingen belemmeren de doeltreffendheid van het onderzoek. Zonder geavanceerde forensische capaciteiten en vaardigheden en betere samenwerking met het bedrijfsleven en tussen nationale autoriteiten blijft cruciaal digitaal bewijsmateriaal ontoegankelijk, wat ernstige gevolgen heeft voor de rechtshandhavingsinspanningen.

- **Gegevens kunnen niet altijd worden gelezen** omdat ze geëncrypteerd zijn. Veel diensten maken nu gebruik van eind-tot-eindencryptie om de vertrouwelijkheid van communicatie en de privacy te beschermen en cyberbeveiliging te waarborgen, maar hierdoor wordt de toegang tot communicatiegegevens voor rechtshandhavingsinstanties sterk bemoeilijkt. Dit betekent dat zelfs legaal onderschepte gegevens vaak niet kunnen worden ontcijferd. Zonder de mogelijkheid om deze gegevens te lezen, blijft belangrijk bewijsmateriaal verborgen, waardoor het veel moeilijker wordt om strafbare feiten te onderzoeken.

[9] SIRIUS Cross-Border Access to Electronic Evidence (Sirius-project), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Gegevens kunnen niet altijd worden geanalyseerd**, omdat bv. de nodige technologie en/of personele middelen niet altijd beschikbaar zijn om grote hoeveelheden gegevens te screenen of in beslag genomen gegevens te filteren en te analyseren op een doeltreffende manier die verenigbaar is met de fundamentele waarden van de EU en de rechtskaders van de EU en de lidstaten.

- **Gegevens kunnen niet worden verkregen** als gevolg van wetsconflicten tussen rechtsgebieden. Gegevens steken vaak internationale grenzen over, waardoor er complexe uitdagingen op het gebied van rechterlijke bevoegdheid ontstaan. Verschillende landen hebben uiteenlopende wet- en regelgeving met betrekking tot de toegang tot gegevens, waardoor het moeilijk is om in het buitenland opgeslagen gegevens te verkrijgen. De nieuwe EU-verordening en -richtlijn inzake elektronisch bewijsmateriaal zijn belangrijke stappen om dit te vergemakkelijken, maar er moet nog veel werk worden verzet om deze maatregelen volledig uit te voeren – en zonder volledige uitvoering blijft de toegang tot cruciale gegevens uit andere landen een groot probleem voor de rechtshandhaving.

Dit zijn enkele problemen waarmee rechtshandhavingsinstanties dagelijks worden geconfronteerd.

Criminelen passen hun gedrag voortdurend aan om opsporing te verhinderen. Uit de beschikbare statistieken[10] blijkt dat criminelen in toenemende mate overstappen op rechtmatige eind-tot-eindgeëncrypteerde platforms. Zodra er doeltreffende tegenmaatregelen worden gevonden, is de kans echter groot dat zij opnieuw op andere communicatiekanalen overstappen. Daarom is het van het grootste belang dat rechtshandhavingsinstanties, bijgestaan door deskundigen uit alle betrokken gemeenschappen, technologische ontwikkelingen kunnen volgen en kunnen anticiperen op veranderingen in crimineel gedrag, zoals die welke verband houden met 6G, het internet der dingen (IoT) en satellietcommunicatie. Bovendien moeten de capaciteiten die succesvolle operaties tegen specifieke criminele communicatiediensten (bv. EncroChat, Ghost ECC) mogelijk hebben gemaakt, worden gehandhaafd en aangepast om het hoofd te bieden aan soortgelijke toekomstige uitdagingen.

[10] Europol IOCTA 2024.

Rechtshandhavingsinstanties hebben steeds meer rechtmatige toegang tot digitale informatie nodig. Aangezien criminelen steeds meer gebruikmaken van onlinediensten, neemt het aantal verzoeken om gegevens aan aanbieders van onlinediensten toe: dat aantal is tussen 2017 en 2022 verdrievoudigd[11]. Communicatiegegevens (zowel metagegevens als inhoudelijke gegevens) zijn van cruciaal belang voor veel strafrechtelijke onderzoeken. Toegang tot digitaal bewijsmateriaal wordt geacht een belangrijke rol te spelen in 85 % van de onderzoeken[12]. Met de nieuwe reeks regels inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal zullen de bevoegde autoriteiten beter in staat zijn toegang tot die gegevens te krijgen. Deze regels kunnen echter alleen uitwerking hebben als de gegevens in een leesbaar formaat beschikbaar zijn. Ook de toegang tot gegevens die zijn opgeslagen in in beslag genomen apparaten en de legale interceptie van communicatie blijven zowel juridisch als praktisch opmerkelijk problematisch. Voor het doeltreffend onderscheppen van gegevens in doorvoer in grensoverschrijdende zaken, kunnen de lidstaten om justitiële samenwerking verzoeken via de Overeenkomst betreffende de wederzijdse rechtshulp[13] en het Europees onderzoeksbevel[14]. Deze instrumenten zijn echter hoofdzakelijk ontworpen met het oog op de uitwisseling van fysiek bewijsmateriaal en zijn misschien niet zo doeltreffend in de context van de technologische ontwikkelingen.

Rechtmatige toegang moet onderworpen zijn aan strikte voorwaarden, die zijn vastgelegd in het nationale, EU- en internationale recht, en die toegang moet worden geregeld in transparante procedures die voorzien in een verantwoordingsplicht en die onder meer gericht zijn op het voorkomen van onrechtmatige openbaarmaking van bedrijfsgeheimen en, in het geval van rechtmatige openbaarmaking, op het nemen van passende maatregelen om de vertrouwelijkheid ervan te waarborgen.

Rechtmatige toegang moet volledig in overeenstemming zijn met de beginselen van noodzakelijkheid en evenredigheid, en moet zo nodig worden goedgekeurd door een rechter of een onafhankelijke autoriteit. De toegang tot gegevens moet gepaard gaan met robuuste privacybescherming en cyberbeveiligingsmaatregelen (bv. encryptie, firewalls, antivirus- en antimalwaresoftware). Het beperken van de toegang tot gegevens tot wat noodzakelijk is voor een onderzoek, draagt bij tot de bescherming van de privacy van individuele gebruikers.

---

11 Sirius-project.

12 Effectbeoordeling door de Commissie van de voorstellen voor een verordening inzake elektronisch bewijsmateriaal en een richtlijn inzake elektronisch bewijsmateriaal (17 april 2018).

13 Wederzijdse rechtshulp - normen van de Raad van Europa - PC-OC (coe.int).

14 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32014L0041.

Hoewel rechtmatige toegang tot gegevens voor rechtshandhavingsdoeleinden essentieel is om onze burgers het hoogst mogelijke beveiligingsniveau te bieden, mag dit niet ten koste gaan van de grondrechten of de cyberbeveiliging van systemen en producten. Er mag geen sprake zijn van een compromis tussen de bescherming van de persoonlijke integriteit en veiligheid van personen enerzijds en hun rechten anderzijds; er moet een evenwicht worden gevonden dat ervoor zorgt dat het ene het andere niet aantast. Zowel de EU als de lidstaten hebben de plicht ervoor te zorgen dat burgers een hoog niveau van bescherming van hun grondrechten kunnen genieten en dat zij zich dag in dag uit veilig voelen. Technologische ontwikkelingen mogen geen veilige haven voor criminelen creëren: indien er een redelijk vermoeden bestaat dat een strafbaar feit is gepleegd of zal worden gepleegd, moeten de rechtshandhavingsinstanties toegang hebben tot instrumenten waarmee zij de betrokken gegevens kunnen raadplegen.

In het Europees Verdrag tot bescherming van de rechten van de mens, de nationale grondwetten en het Handvest van de grondrechten van de Europese Unie wordt erkend dat iedereen recht heeft op een privéleven en dat dit de communicatie van een persoon omvat. In het Handvest van de grondrechten van de Europese Unie is ook het recht op gegevensbescherming vastgelegd. Het recht op privacy en het recht op bescherming van persoonsgegevens hebben geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving[15]. Overheidsinstanties mogen zich niet mengen in de uitoefening van deze rechten, ***tenzij die inmenging in overeenstemming is met de wet, de wezenlijke inhoud van de rechten onverlet laat en in een democratische samenleving noodzakelijk en evenredig is.*** Onder die voorwaarden kunnen het recht op privacy en het recht op bescherming van persoonsgegevens worden beperkt, onder meer in het belang van de nationale en openbare veiligheid en voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

Een sterke verantwoordingsplicht is van cruciaal belang. In onze democratische samenlevingen is het de verantwoordelijkheid van de wetgevers om de voorwaarden voor de verantwoordingsplicht vast te leggen en daarbij een hoog niveau van privacy en veiligheid te waarborgen. ***Privacy en veiligheid sluiten elkaar niet uit***.

Teneinde innovatie en sterke cyberbeveiliging te bevorderen, moeten, in samenwerking met alle belanghebbenden, met inbegrip van het bedrijfsleven, oplossingen worden ontwikkeld om in gerechtvaardigde gevallen rechtmatige toegang te waarborgen. ***Deze oplossingen moeten in overeenstemming zijn met alle desbetreffende behoeften en vereisten en de ontwikkeling ervan mag niet volledig aan technologische ondernemingen worden overgelaten.***

[15] Arrest van 30 april 2024, *La Quadrature du Net e.a.*, zaak C-470/21, ECLI:EU:C:2024:370, punt 70.

Voordat verdere stappen kunnen worden ondernomen, moeten technische beoordelingen worden uitgevoerd, zodat kan worden tegemoetgekomen aan de punten van zorg van sommige deskundigen op het gebied van cyberbeveiliging, met name met betrekking tot de complexiteit van enerzijds het waarborgen van rechtmatige toegang en anderzijds het handhaven van sterke cyberbeveiliging. ***De cyberbeveiliging van producten en diensten en de rechtmatige toegang tot gegevens vloeien beide voort uit wettelijke verplichtingen en moeten naast elkaar kunnen bestaan.*** De vereisten inzake rechtmatige toegang moeten worden uitgevoerd op basis van duidelijke normen die door alle belanghebbenden (onder meer vertegenwoordigers van het bedrijfsleven, deskundigen op het gebied van gegevensbescherming en cyberbeveiliging, en rechtshandhavers) zijn ontwikkeld, rekening houdend met de desbetreffende wettelijke vereisten en op basis van naar behoren beoordeelde potentiële oplossingen, zodat wordt gewaarborgd dat rechtmatige toegang geen afbreuk doet aan de veiligheid van producten en diensten.

Veel ondernemingen en dienstverleners aarzelen om samen te werken met rechtshandhavingsinstanties vanwege de rechtsonzekerheid waarmee vrijwillige maatregelen gepaard gaan en het risico van mogelijke negatieve reacties bij hun gebruikers. Deze terughoudendheid belemmert onderzoeken. Bovendien kan de perceptie dat gebruikers prioriteit geven aan privacy boven openbare veiligheid ertoe leiden dat actoren uit de sector terughoudend zijn om communicatiekanalen te openen met rechtshandhavingsinstanties en aangepaste mechanismen voor rechtmatige toegang te creëren. Er is een duidelijk rechtskader voor rechtmatige toegang tot gegevens nodig om dit probleem aan te pakken. In de bestaande wetgeving zijn er aanzienlijke belemmeringen die het verlenen van rechtmatige toegang, met name op vrijwillige basis, bemoeilijken.

De samenwerking tussen ondernemingen en rechtshandhavingsinstanties is ondermaats en gebrekkig en moet worden aangevuld met duidelijke regels. ***Zonder duidelijke, afdwingbare wettelijke verplichtingen zijn ondernemingen vaak niet in staat om rechtshandhavingsinstanties te helpen bij de toegang tot gegevens***.

Bij gebrek aan doeltreffende oplossingen om rechtmatige toegang te waarborgen, ***worden op kwetsbaarheid gebaseerde oplossingen vaak als de enige optie beschouwd***.

Wanneer onderschepte gegevens (en mogelijk andere gegevens die uit een apparaat zijn geëxtraheerd) worden verwerkt met instrumenten die zijn ontworpen door particuliere ondernemingen, hebben de nationale autoriteiten, ongeacht de garanties die deze ondernemingen bieden, niet echt zicht op welke gegevens er worden gescreend en hoe, en kunnen zij niet anders dan voortgaan op de certificaten van de overheid van het land waar de ondernemingen die de onderscheppingsdienst aanbieden, gevestigd zijn. Het feit dat de gebruikte kwetsbaarheid geheim moet worden gehouden om de doeltreffendheid van de instrumenten/diensten te handhaven, verergert dit probleem. Dit probleem is bijzonder zorgwekkend wanneer de aanbieder buiten de EU is gevestigd.

Tot slot, maar daarom niet minder belangrijk, hebben particuliere ondernemingen die met hun diensten ingrijpende onderzoekstechnieken ondersteunen, er alle belang bij hun winst te maximaliseren. Zij kunnen derhalve beslissen hun instrumenten te verkopen aan niet-democratische regimes (zoals dat het geval was bij het Hacking Team-schandaal[16]).

Anderzijds kan een problematische toegang tot gegevens ***rechtshandhavingsinstanties ertoe aanzetten ingrijpendere onderzoeksmaatregelen te nemen***. In dergelijke gevallen zijn de rechtshandhavingsinstanties genoodzaakt hun toevlucht te nemen tot maatregelen die meer in de persoonlijke levenssfeer ingrijpen, zoals fysiek toezicht in plaats van raadpleging van geolocatiegegevens en huiszoekingen in plaats van legale interceptie.

Het onvermogen van rechtshandhavingsinstanties om toegang te krijgen tot gegevens kan leiden tot aanzienlijk vertrouwensverlies van het publiek ten aanzien van het gerechtelijk apparaat. Wanneer onderzoeken worden vertraagd of geschaad, kunnen burgers het gevoel krijgen dat het gerechtelijk apparaat niet naar behoren werkt. Door dit tanende vertrouwen wordt mogelijk de openbare orde ondermijnd en is het publiek minder geneigd om bij te dragen aan de rechtshandhaving.

Tot slot ***zorgt rechtmatige toegang ervoor dat rechtshandhavingsinstanties bewijsmateriaal kunnen verzamelen om recht te doen aan slachtoffers en hen te beschermen tegen verdere schade***. Gegevens kunnen belangrijke aanwijzingen bevatten voor het onthullen en vervolgen van alle soorten strafbare feiten, zowel offline als online. Personen kunnen worden blootgesteld aan ernstige vormen van cyberpesten, identiteitsdiefstal, fraude enz. als gevolg van het criminele misbruik van digitale technologieën, diensten en communicatie. Deze ervaringen kunnen ernstige emotionele en mentale gevolgen hebben voor de slachtoffers en vergroten de bestaande ongelijkheden en kwetsbaarheden.

[16] Zie https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

In elk strafrechtelijk onderzoek is bewijsmateriaal nodig om de dader te identificeren of om zijn of haar verantwoordelijkheid aan te tonen in een rechtbank. Het kan ook helpen een burger vrij te spreken als hij of zij ten onrechte is beschuldigd. Als rechercheurs en openbare aanklagers geen toegang hebben tot de nodige informatie, zijn zij mogelijk niet in staat vooruitgang te boeken in hun onderzoek en de dader te identificeren, wat extra leed en financiële verliezen voor het slachtoffer veroorzaakt en het vertrouwen in het gerechtelijk apparaat uitholt. Traditioneel fysiek bewijs alleen volstaat niet altijd om verbanden te leggen en aanwijzingen te vinden. ***Rechtshandhaving en justitie moeten worden klaargemaakt voor het digitale tijdperk. Alleen dan zullen zij onze samenlevingen en economieën volledig kunnen beschermen*** tegen toenemende dreigingen als gevolg van cyberaanvallen en hybride dreigingen, en tegen georganiseerde criminele activiteiten.

Kortom, als rechtshandhavingsinstanties geen doeltreffende toegang hebben tot gegevens, zijn zij minder goed in staat om de veiligheid te waarborgen en de plegers van de ernstigste strafbare feiten aan te houden. ***Rechtshandhavingsinstanties moeten rechtmatige en strikt gecontroleerde doeltreffende toegang tot gegevens krijgen, met robuuste privacybescherming en cyberbeveiligingswaarborgen, om strafbare feiten te voorkomen, op te sporen, te onderzoeken en te vervolgen, zodat zij de veiligheid kunnen waarborgen en EU-burgers in veiligheid kunnen leven en gerechtigheid kunnen verkrijgen voor tegen hen gepleegde strafbare feiten.***

Hoofdstuk I: digitaal forensisch onderzoek

WAAR GAAT HET OM?

Digitaal forensisch onderzoek heeft betrekking op het verzamelen, analyseren en bewaren van digitaal bewijsmateriaal (zowel communicatiemetagegevens als inhoudelijke gegevens) dat in digitale vorm op een elektronisch apparaat is opgeslagen, waaronder informatie op harde schijven van computers, in mobiele telefoons, op slimme apparaten, in voertuignavigatiesystemen en elektronische deursloten, in de cloud opgeslagen gegevens en informatie in andere digitale apparaten.

Naarmate het moeilijker wordt om toegang te krijgen tot communicatiegegevens, wordt het extraheren van informatie uit in beslag genomen apparaten (of uit netwerken van verbonden apparaten) steeds belangrijker in het kader van strafrechtelijk onderzoek. Dankzij toegang tot inactieve gegevens in apparaten kunnen rechtshandhavingsinstanties betere informatie verzamelen over bijvoorbeeld de identiteit van de leden van een georganiseerde criminele organisatie, dan bij andere technieken zoals legale interceptie. Sommige deskundigen stellen dat zij niet vooraf kunnen weten welke gegevens belangrijk zijn voor een specifiek onderzoek: zelfs informatie die aanvankelijk irrelevant lijkt, kan van vitaal belang worden naarmate het onderzoek vordert. Toegang tot alle gegevens op een apparaat kan ook belangrijk zijn om de onschuld van een verdachte te bevestigen en de rechten van een verweerder te beschermen[17]. Bovendien moeten onderzoeksmethoden altijd evenredig zijn.

Het chronische **gebrek aan middelen** en capaciteiten waarmee rechtshandhavingsinstanties op dit gebied worden geconfronteerd, wordt nog verergerd door de uitrol van nieuwe technologieën (bv. nieuwe soorten apparaten, IoT en cloudcomputing), waarvoor nieuwe vaardigheden en instrumenten nodig zijn. Hoewel de agentschappen en instellingen van de lidstaten reeds over aanzienlijke deskundigheid op het gebied van digitaal forensisch onderzoek beschikken, is die kennis versnipperd en blijft deze geïsoleerd omdat er geen goede mechanismen bestaan voor het delen en verspreiden van capaciteiten.

[17] Een deskundige haalde een zaak aan waarin de analyse van de activiteit van het apparaat van wezenlijk belang was om aan te tonen dat de verdachte niet betrokken kon zijn geweest bij een moord.

Het gebrek aan vergelijkbare capaciteiten bij laboratoria voor digitaal forensisch onderzoek en het algemene gebrek aan **forensische standaardprocedures** en mechanismen die de **erkenning van de vaardigheden en vakbekwaamheid van deskundigen op het gebied van digitaal forensisch onderzoek** mogelijk maken, kunnen grensoverschrijdende samenwerking belemmeren.

De GHN-deskundigen lieten er geen twijfel over bestaan:standaard**encryptie** van gegevens op apparaten is een belangrijke uitdaging voor rechtshandhavingsinstanties. Gegevens die zijn opgeslagen op bepaalde soorten moderne apparaten die zijn beschermd door cryptochips[18] of door sterke encryptiealgoritmen en complexe wachtwoorden, zijn niet toegankelijk voor rechtshandhavingsinstanties, zelfs niet met behulp van de krachtigste decryptieplatforms. Encryptie en andere cyberbeveiligings- en privacygerelateerde maatregelen zijn noodzakelijk om informatiesystemen en communicatie- en persoonsgegevens te beschermen, maar deze maatregelen – en met name het toenemende gebruik van standaardencryptie – leiden ertoe dat rechtshandhavingsinstanties moeilijker bewijsmateriaal kunnen verzamelen.

De lidstaten beschikken op dit gebied over beperkte **deskundigheid en capaciteiten**: bijna allemaal geven zij aan niet over de technische oplossingen te beschikken om tegemoet te komen aan de behoeften van beroepsbeoefenaars, en de overgrote meerderheid is van oordeel dat hun vaardigheden en financiële middelen ontoereikend zijn. De capaciteiten van de rechtshandhavingsinstanties om op in beslag genomen apparaten opgeslagen informatie te decrypteren, verschillen aanzienlijk van lidstaat tot lidstaat, variërend van een succespercentage van 15-20 % tot meer dan twee derde. Zij blijken bovendien doorgaans ondoeltreffend bij het decrypteren van gegevens die zijn beveiligd door sterke wachtwoorden en in het geval van bestanden die in speciale geëncrypteerde kluizen worden bewaard. Decryptie, indien al succesvol, komt ook vaak te laat. Decryptieapparatuur is duur en zeer gespecialiseerd, en de hardware verbruikt veel capaciteit.

De meeste afdelingen voor digitaal forensisch onderzoek van rechtshandhavingsinstanties zijn afhankelijk van commerciële oplossingen om toegang te krijgen tot gegevens op apparaten, wat extra problemen met zich meebrengt: deze oplossingen kunnen amper gelijke tred houden met de technologische ontwikkelingen en zijn snel verouderd; de hoge licentiekosten leiden tot een aanzienlijke beperking van het aantal gemachtigde gebruikers, en de oplossingen worden vaak buiten Europa ontwikkeld en zijn mogelijk slecht afgestemd op de behoeften van de rechtshandhavingsinstanties van de EU of voldoen mogelijk niet aan de EU-normen inzake verantwoordingsplicht voor digitaal forensisch onderzoek.

[18] Zoals de T2-beveiligingschip in recente laptops van Apple.

Vaak hebben rechtshandhavingsinstanties geen andere keus dan **kwetsbaarheden** te benutten om zich toegang te verschaffen tot decryptiesleutels op apparaten. Dergelijke onderzoekstechnieken moeten echter verzoenbaar zijn met de in de verordening cyberweerbaarheid vastgelegde doelstelling om hardware en software veiliger te maken. Regelingen voor het beheer en de bekendmaking van kwetsbaarheden zouden de onbedoelde gevolgen van die technieken verlichten. De deskundigen hebben alternatieve oplossingen overwogen, zoals het verplichten van verdachten om de elementen die nodig zijn voor de toegang tot de betrokken apparaten (bv. wachtwoorden) over te dragen aan de met het onderzoek belaste autoriteiten. De in die gevallen toepasselijke nationale rechtskaders verschillen aanzienlijk, en slechts drie lidstaten hebben aangegeven dat zij specifieke wettelijke bepalingen hebben die een verdachte verplichten toegang te verlenen tot decryptiesleutels of tot de gedecrypteerde gegevens[19]. Sommige lidstaten verplichten verdachten om bepaalde biometrische gegevens (bv. een vingerafdruk) beschikbaar te stellen en aldus toegang te verlenen tot een apparaat. In andere gevallen moeten verdachten hun wachtwoord geven. In het algemeen blijft dit een gebied dat verder moet worden geëvalueerd.

Sommige van de hierboven genoemde kwesties kunnen deels worden verholpen door **onderlinge uitwisseling van de capaciteiten van de lidstaten**, met inachtneming van hun exclusieve bevoegdheid op het gebied van nationale veiligheid. Deze oplossing wordt echter genegeerd, soms als gevolg van juridische beperkingen (in zeven lidstaten zijn er beperkingen voor het delen van instrumenten, terwijl vijf lidstaten beperkingen hebben ondervonden bij het gebruik van instrumenten die door andere lidstaten worden gedeeld), maar meer in het algemeen vanwege het gebrek aan gevestigde mechanismen voor het delen van instrumenten of de gezamenlijke aankoop van licenties.

In het verleden beschikten de rechtshandhavingsinstanties over duidelijke **communicatiekanalen met fabrikanten, dienstverleners en leveranciers**. Hierdoor konden zij samenwerkingsprotocollen vaststellen, waardoor zij een beter inzicht kregen in nieuwe technologische ontwikkelingen en dientengevolge gemakkelijker rechtshandhavingsmaatregelen konden nemen en tegelijkertijd de cyberbeveiliging konden waarborgen. Door het hoge tempo waaraan nieuwe technologieën worden uitgerold en nieuwe ondernemingen op de markt komen, zijn de omstandigheden veranderd en wordt er niet langer samengewerkt met het bedrijfsleven.

Indien er passende normen zouden worden vastgesteld, kunnen de productprotocollen en de technische architectuur zodanig worden ontworpen dat in een vroeg stadium rekening wordt gehouden met de bezorgdheden en de technische vereisten van rechtshandhavingsinstanties. De **rechtshandhavingsinstanties zijn echter onvoldoende vertegenwoordigd in de desbetreffende normalisatie-instellingen**, hetgeen afbreuk doet aan hun vermogen om effectief deel te nemen aan de ontwikkeling van de toekomstige technologische normen.

---

[19] Eurojust, Justitiële Monitor Cybercriminaliteit (uitgave 4), december 2018, blz. 34, http://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

MOGELIJKE OPLOSSINGEN

I. De inspanningen voor capaciteitsopbouw op het gebied van digitale forensische instrumenten opvoeren en rationaliseren

De lidstaten beschikken reeds over de deskundigheid en de capaciteiten om digitaal forensisch onderzoek uit te voeren. Door hun technische oplossingen te delen en onderling uit te wisselen, kunnen de bevoegde nationale instellingen en autoriteiten echter profiteren van de ervaring van andere agentschappen en aanzienlijke schaalvoordelen behalen, waardoor er minder financiële middelen nodig zijn. De lidstaten kunnen desbetreffende oplossingen nader onderzoeken, zowel op het gebied van digitale forensische instrumenten als wat betreft opleiding en de ontwikkeling van vaardigheden.

Aanbevelingscluster 1

Om de samenwerking te verbeteren en de collectieve capaciteit op het gebied van digitaal forensisch onderzoek te versterken, bevelen de deskundigen het volgende aan:

1. *de bestaande digitale forensische netwerken in kaart brengen en verbinden en een secretariaat oprichten [aanbeveling 1];*
2. *kennis toegankelijker maken en verspreiden onder deskundigen[aanbeveling 1];*
3. *nadenken over mechanismen voor het bundelen van kennis [aanbeveling 2];*
4. *de financiering voor onderzoek en ontwikkeling verhogen, met duidelijke doelstellingen [aanbeveling 4];*
5. *het Europol-instrumentenregister promoten als centraal knooppunt voor het delen van instrumenten [aanbeveling 4];*
6. *het delen van oplossingen en digitale forensische instrumenten tussen de lidstaten bevorderen in een klimaat van vertrouwen (met inachtneming van de nationale regels) [aanbeveling 2];*
7. *op EU-niveau een mechanisme ontwikkelen voor de gezamenlijke aankoop van licenties voor digitale forensische instrumenten, zodat deze tussen de lidstaten gedeeld kunnen worden [aanbeveling 3];*
8. *de samenwerking met producenten en ontwikkelaars van digitale forensische instrumenten bevorderen om de structuur en het formaat van de door rechtshandhavingsinstanties verkregen gegevens te stroomlijnen door het gebruik van die instrumenten, idealiter volgens overeengekomen normen [aanbeveling 12];*
9. *een mechanisme/regeling opzetten voor de evaluatie en – indien relevant – voor de certificering van commerciële digitale forensische instrumenten op EU-niveau, rekening houdend met mogelijke negatieve gevolgen voor onderzoek en vervolging, zoals het verhogen van onnodige lasten [aanbeveling 5].*

Verschillende organisaties, netwerken, verenigingen en projecten brengen beroepsbeoefenaars en verschillende categorieën partners samen om de capaciteit van de rechtshandhavingsinstanties in de EU op het gebied van digitale onderzoeken te vergroten:

- het *Europees netwerk van forensische instituten* (Enfsi)[20] is het belangrijkste Europese netwerk dat zich (onder meer) met digitaal forensisch onderzoek bezighoudt. 73 leden uit 39 landen komen samen in werkgroepen over bijvoorbeeld forensische informatietechnologie en digitale beeldvorming;

- de Europese vereniging voor de ontwikkeling van technologieën op het gebied van cybercriminaliteitsbestrijding (*European Anti-Cybercrime Technology Development Association* (EACTDA))[21] brengt rechtshandhavingsinstanties, onderzoeks- en technologieorganisaties, industriële partners en de academische wereld uit tal van lidstaten samen met als doel een bredere toepassing van de resultaten van beveiligingsonderzoeksprojecten en de levering van volledig geteste en operationele software-instrumenten zonder licentiekosten en met toegang tot de broncode voor openbareveiligheidsorganisaties van de EU;

- het Europees Bureau voor fraudebestrijding (OLAF) biedt nationale rechtshandhavingsinstanties sinds 2007 *specifieke opleidingen voor digitaal forensisch onderzoek en digitale analisten* aan, met bijzondere aandacht voor fraude, corruptie en andere onwettige activiteiten die de financiële belangen van de Europese Unie schaden. Jaarlijks worden ongeveer 175 deskundigen op het gebied van digitaal forensisch onderzoek opgeleid, waardoor een solide gemeenschap van deskundigen op dit gebied wordt opgebouwd;

- andere projecten, zoals *CYCLOPES*[22] en *I-LEAD*[23], zijn geen permanente structuren, maar brengen niettemin deskundigen samen en leveren relevante kloofanalysen.

De bestaande permanente netwerken volstaan echter niet om de eenheden van EU-rechtshandhavingsinstanties die belast zijn met digitaal forensisch onderzoek en organisaties die nauw met hen samenwerken (bijvoorbeeld het Centre for Cybersecurity and Cybercrime Investigation van het University College Dublin (UCD) of het Litouwse Cybercrime Center of Excellence for Training, Research and Education) samen te brengen.

---

20 https://enfsi.eu/.
21 https://www.eactda.eu/index.html.
22 https://www.cyclopes-project.eu/.
23 https://cordis.europa.eu/project/id/740685/en.

Europol (met name het innovatielab van Europol, samen met het Europees Centrum voor de bestrijding van cybercriminaliteit) werkt al tot op zekere hoogte samen met alle genoemde netwerken en heeft bewezen dat het een aanzienlijk aantal beroepsbeoefenaars kan samenbrengen, bijvoorbeeld in de vorm van de kerngroepen van de Europese clearingraad voor innovatie (European Clearing Board for Innovation, EuCB), door het organiseren van het *Forensics Experts Forum (forum van forensische deskundigen)*[24] en door deskundigen in contact te brengen met relevante partners, bijvoorbeeld via het *Cyber Innovation Forum (cyberinnovatieforum)*[25].

Europol biedt ook een kant-en-klare infrastructuur – het Europol-platform voor experts (EPE) – die samenwerking en kennisuitwisseling tussen deskundigen over specifieke onderwerpen mogelijk maakt.

Kernactie: de GHN-deskundigen roepen op tot versterking van de capaciteiten van Europol op het gebied van digitaal forensisch onderzoek

Actoren: Europol, Europese Commissie, lidstaten	*Tijdschema: 2028*	*Begroting: op een later tijdstip te bespreken, afhankelijk van het resultaat van de lopende besprekingen over het volgende MFK*

- In het kader van de aanzienlijke versterking van Europol die in de politieke beleidslijnen voor de Europese Commissie 2024-2029 is aangekondigd, roepen de GHN-deskundigen op tot versterking van de capaciteit van Europol om de lidstaten te helpen **middelen, kennis en deskundigheid te bundelen en oplossingen en digitale forensische instrumenten te delen** in een klimaat van vertrouwen. Soevereine instrumenten en instrumenten die uitsluitend voor nationale veiligheidsdoeleinden worden gebruikt en/of ontwikkeld, moeten worden uitgesloten.

- De GHN-deskundigen verzoeken Europol **als knooppunt te fungeren** voor toegang tot operationele expertise op dit gebied, en eventueel **een met Sirius vergelijkbaar project op te zetten op het gebied van digitaal forensisch onderzoek** om de uitwisseling van kennis, deskundigheid en beste praktijken te vergemakkelijken.

- De GHN-deskundigen verzoeken Europol zijn rol in **coördinerende organisaties en projecten** die bijdragen tot kennisverwerving op het gebied van digitaal forensisch onderzoek op EU-niveau te versterken, onder leiding van de EuCB en rekening houdend met de input van andere bevoegde agentschappen.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference.
[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024.

Er bestaan verschillende financiële instrumenten ter ondersteuning van het onderzoek en de ontwikkeling van instrumenten op het gebied van digitaal forensisch onderzoek.

- In het kader van het *Fonds voor interne veiligheid (Internal Security Fund, ISF)* maakt de Europese Commissie regelmatig open oproepen tot het indienen van voorstellen op het gebied van cybercriminaliteit en digitale onderzoeken bekend. Ondanks de vrij beperkte begroting (ongeveer 15 miljoen EUR onder het huidige MFK), zijn de in het kader van deze oproepen geselecteerde projecten doelgericht en succesvol gebleken.

  Ongeveer twee derde van de ISF-begroting wordt toegewezen via gedeeld beheer, waarbij de lidstaten kiezen welke projecten worden gefinancierd en de verantwoordelijkheid voor het dagelijks beheer op zich nemen. De lidstaten kunnen derhalve in het kader van hun respectieve nationale programma's projecten op het gebied van digitaal forensisch onderzoek ondersteunen.

- De cluster *Civiele veiligheid voor de samenleving* van *Horizon Europa*, die een totale begroting van 1,596 miljard EUR over zeven jaar heeft, is erop gericht veilige Europese samenlevingen te bevorderen in een context van ongekende transformaties en wereldwijd toenemende onderlinge afhankelijkheden en dreigingen, en de Europese cultuur van vrijheid en recht daarbij steviger te verankeren. De afgelopen jaren zijn in het kader van dat programma verschillende onderzoeksprojecten ondersteund, zoals FORMOBILE[26] en EXFILES[27], die beroepsbeoefenaars bij hun dagelijkse activiteiten hebben ondersteund.

- Het programma *Digitaal Europa* is het belangrijkste financieringsinstrument van de EU om de digitale infrastructuur van de EU te verbeteren door middel van diverse initiatieven. Het programma, dat een totale begroting heeft van 7,5 miljard EUR voor de periode 2021-2027, voorziet in aanzienlijke middelen voor cyberbeveiliging, en omvat ook digitaal forensisch onderzoek.

[26] FORMOBILE – Van mobiele telefoons tot de rechtbank – Een alomvattende FORensisch-onderzoeksketen gericht op mobiele (MOBILE) toestellen (https://cordis.europa.eu/project/id/832800).

[27] EXFILES – Europa bestrijdt misdaad en terrorisme (https://exfiles.eu/).

Het decryptieplatform van Europol is een vlaggenschipproject van het ISF. Dit platform, dat Europol in 2020 heeft opgezet in nauwe samenwerking met het Gemeenschappelijk Centrum voor onderzoek (Joint Research Centre, JRC) van de Europese Commissie, ondersteunt nationale rechtshandhavingsinstanties door hun digitaal bewijsmateriaal te decrypteren. Het platform is erop gericht rechtshandhavingsinstanties een duurzame oplossing te bieden voor de toegang tot de technische en IT-middelen die zij nodig hebben. De afgelopen jaren is het platform in tal van belangrijke zaken gebruikt en heeft het in bijna de helft daarvan belangrijke resultaten opgeleverd, met verschillende succesverhalen tot gevolg. In 2023 heeft het platform met succes 37 onderzoeken (naar seksuele uitbuiting van kinderen, terrorisme, cybercriminaliteit, georganiseerde criminaliteit, drugssmokkel en fraude, alsmede spraakmakende financiële onderzoeken) ondersteund, waaronder onderzoeken met hoge prioriteit, zoals die naar SkyECC en EncroChat. Het platform is een essentieel instrument geworden voor rechtshandhavingsinstanties, maar het volstaat niet om alle decryptieproblemen waarmee de EU-autoriteiten te maken hebben, op te lossen.

Kernactie: de GHN-deskundigen roepen ertoe op het gebruik van de EU-decryptiecapaciteiten verder te ontwikkelen en te bevorderen

Actoren: Europese Commissie, Europol	*Tijdschema: 2028*	*Begroting: te bepalen door de lidstaten (bv. in het kader van de nationale programma's van het ISF)*

- De GHN-deskundigen verzoeken de Europese Commissie om, met inachtneming van de exclusieve bevoegdheid van de lidstaten op het gebied van nationale veiligheid, het vermogen van de nationale autoriteiten om contextuele informatie van hoge kwaliteit te verzamelen, te ondersteunen door middel van specifieke financiering (bv. in het kader van de nationale programma's van het ISF), alsook de uitwisseling van beste praktijken te bevorderen, zodat die autoriteiten de efficiëntie van het decryptieplatform van Europol kunnen helpen verhogen.

- De GHN-deskundigen verzoeken de Europese Commissie de investeringen van Europol in het handhaven van de technische capaciteiten en het versterken van de decryptiecapaciteiten te ondersteunen, zodat gelijke tred kan worden gehouden met de technologische ontwikkelingen en het onderzoek naar kwantumcryptografie in aanmerking wordt genomen.

- De GHN-deskundigen verzoeken de Europese Commissie de lidstaten financieel te ondersteunen bij de ontwikkeling van **nationale en regionale decryptiecapaciteiten**, als aanvulling op de inspanningen van Europol.

De bestaande financieringsprogramma's van de EU bieden aanzienlijke steun voor rechtshandhaving. Een verdere stroomlijning van deze mogelijkheden zou de capaciteit van de afdelingen voor digitaal forensisch onderzoek helpen vergroten en het insluitingseffect en de afhankelijkheid van rechtshandhavingsinstanties van buiten de EU ontwikkelde "black box"-instrumenten (d.w.z. instrumenten die gegevens verwerken zonder dat betrouwbare autoriteiten kunnen nagaan hoe zij functioneren) verkleinen.

De stappen in de activiteitencyclus (onderzoek, ontwikkeling, toepassing) die moeten worden ondernomen om een concrete meerwaarde voor rechtshandhavingsinstanties te creëren, worden ondersteund door verschillende regelingen. Om de mogelijkheden die op EU-niveau worden geboden, ten volle te benutten, moeten nationale overheden, rechtshandhavingsinstanties en beroepsbeoefenaars op de hoogte zijn van de functies en doelstellingen van elk specifiek programma en mechanisme.

Horizon Europa heeft verschillende succesvolle projecten ondersteund, met actieve deelname van rechtshandhavers. Horizon Europa is echter een onderzoeksprogramma en de verwachtingen met betrekking tot de mate waarin de ontwikkelde instrumenten operationeel zijn, moeten worden bijgesteld.

Het project *Tools4LEAs*, gefinancierd door het ISF en beheerd door EACTDA, is gericht op een bredere toepassing van de resultaten van beveiligingsonderzoeksprojecten en de levering van volledig geteste en operationele software-instrumenten zonder licentiekosten en met toegang tot de broncode voor EU-organisaties op het gebied van openbare veiligheid. *Tools4LEAs* is het meest geschikt om voort te bouwen op de resultaten van onderzoeksprojecten met het oog op de levering van operationele instrumenten. Europol is betrokken bij het *Tools4LEAs*-project en stuurt, samen met alle eindgebruikers die lid zijn van EACTDA, de werkzaamheden ervan aan.

De EuCB heeft meer dan 15 kerngroepen van lidstaten opgericht om nieuwe technologieën te exploiteren en samen innovatieve instrumenten te ontwikkelen. De lidstaten hebben een beroep gedaan op de kerngroepen van de EuCB om een deel van de ontwikkeling van de met ISF-subsidies gefinancierde innovatieve instrumenten, zoals MARIT-D, ProfID en webcrawlers, te coördineren. Kerngroepen vormen een ideaal kader waarbinnen de lidstaten de cocreatie van digitale onderzoeksinstrumenten kunnen coördineren.

Via gerichte *oproepen tot het indienen van voorstellen in het kader van het ISF* blijft de Europese Commissie projecten financieren die aanzienlijk bijdragen tot het welslagen van operationele acties. Zo bracht het Cerberus-project de kwetsbaarheden in het EncroChat-systeem aan het licht, waardoor de Franse Gendarmerie, ondersteund door het Nederlands Forensisch Instituut en het UCD, het kon ontmantelen. Het FREETOOL-project[28], dat wordt geleid door het UCD-centrum voor cyberbeveiliging en onderzoeken op het gebied van cybercriminaliteit, zorgde intussen voor de ontwikkeling van een reeks gratis onderzoeksinstrumenten op het gebied van cybercriminaliteit[29] die zijn toegesneden op specifieke rechtshandhavingsvereisten voor digitale onderzoeken en digitale analyse. Deze instrumenten zijn ontwikkeld in partnerschap met rechtshandhavingsinstanties en staan gratis te hunner beschikking. 3 000 gebruikers van meer dan 100 rechtshandhavingsinstanties uit tientallen rechtsgebieden hebben zich geregistreerd voor toegang tot de instrumenten, die ook door verschillende rechtshandhavingsinstanties op organisatieniveau zijn ingevoerd en gebruikt in belangrijke onderzoeken. Het programma *Justitie* heeft ook betrekking op justitiële samenwerking in strafzaken en kan grensoverschrijdende samenwerking bij het gebruik van digitale onderzoeksinstrumenten bevorderen.

---

28 https://www.ucd.ie/cci/projects/freetool/.

29 De instrumenten bestrijken de verschillende onderzoeksfasen: vergaren van inlichtingen uit open bronnen (Osint) voorafgaand aan het onderzoek, forensisch onderzoek met realtimegegevens, geheugenanalyse, Osint volgend op het onderzoek en behoud van onlinehulpbronnen, automatische opvraging van bestanden/artefacten, forensische rapportage, mediaverwerking, en geolokalisering van artefacten.

Het *Europol-instrumentenregister* (*Europol Tool Repository*, ETR) is geëvolueerd naar een register met meer dan veertig geavanceerde instrumenten die rechtstreekse toegang bieden tot de allernieuwste technologieën voor Europese rechtshandhaving, en maandelijks komen er nieuwe instrumenten bij. Het is dan ook de belangrijkste bron geworden voor beroepsbeoefenaars in de EU die op zoek zijn naar software ter ondersteuning van hun onderzoeken. Het ETR telt momenteel meer dan 2 700 gebruikers en de verschillende instrumenten ervan werden in totaal meer dan 7 800 keer gedownload. De nationale onderzoekseenheden hebben deze instrumenten op grote schaal gebruikt bij talrijke operaties op verschillende criminaliteitsgebieden, zoals mensenhandel, zware en georganiseerde criminaliteit, cybercriminaliteit en online seksueel misbruik van kinderen. Het ETR biedt een directe exploitatiemogelijkheid voor door de EU gefinancierde projecten die concrete en bruikbare resultaten opleveren en waarvan de ontwikkelaars bereid zijn deze in licentie te geven aan Europol voor verspreiding onder alle Europese rechtshandhavingsinstanties. Geselecteerde partners van de projecten INSPECTr, Tools4LEAs en FORMOBILE hebben al instrumenten gedeeld via het ETR. Europol werkt samen met het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol) om gebruikers opleidingen over ETR-instrumenten aan te bieden.

Bovendien moet het programma Digitaal Europa sterker de synergieën en complementariteit bevorderen tussen cyberbeveiliging en de bestrijding van cybercriminaliteit – waarvoor vaak dezelfde digitale forensische instrumenten en technieken worden gebruikt.

Momenteel bestaat er geen mechanisme om ervoor te zorgen dat digitale forensische instrumenten voldoen aan de verantwoordings- en forensische normen binnen de EU. Een dergelijk mechanisme moet voorzien in een technische evaluatie om ervoor te zorgen dat de evenredigheid (d.w.z. bewijzen dat het instrument toegang biedt tot gerichte informatie, waardoor de analyse beperkt blijft tot wat noodzakelijk is), de transparantie en de rechten van de verdediging (d.w.z. aantonen dat het instrument authentieke en nauwkeurige informatie opvraagt waarop de vertegenwoordigers van de verdediging en onafhankelijke forensische deskundigen die in de rechtbank getuigen, kunnen vertrouwen) en andere wettelijke vereisten (bv. naleving van de AI-verordening) volledig worden nageleefd. Dit zou de betrouwbaarheid van het bewijsmateriaal in de rechtbank, zowel nationaal als grensoverschrijdend, vergroten en aldus de grensoverschrijdende samenwerking versterken.

Kernactie: de GHN-deskundigen roepen op tot gerichte financiering van projecten voor onderzoek naar digitale forensische instrumenten en de ontwikkeling en de toepassing ervan

Actoren: Europese Commissie, Europol, lidstaten, EACTDA, Enfsi	*Tijdschema: vanaf 2024*	*Begroting:*

- De GHN-deskundigen verzoeken de lidstaten om **projecten op het gebied van digitaal forensisch onderzoek die in het kader van hun nationale ISF-programma's worden gefinancierd, te integreren in bestaande mechanismen** (bv. Empact) of netwerken (bv. ECTEG, EACTDA), teneinde te profiteren van de ervaring van beroepsbeoefenaars uit andere lidstaten en tegelijkertijd de verspreiding en toepassing van resultaten door andere rechtshandhavingsinstanties te bevorderen.

- De GHN-deskundigen zijn ingenomen met de lopende inspanningen van de Europese Commissie om het onderzoek naar digitale forensische instrumenten en de ontwikkeling en uitrol ervan te ondersteunen door middel van financiering in het kader van de desbetreffende financiële programma's: **Horizon Europa**, **Digitaal Europa** en het **ISF**. Afhankelijk van de beschikbare middelen zal de Europese Commissie in het kader van het ISF om de twee jaar **openbare oproepen tot het indienen van voorstellen** op het gebied van cybercriminaliteit en digitale onderzoeken bekendmaken.

- De GHN-deskundigen zijn ingenomen met de lopende inspanningen van de Europese Commissie om in het kader van het ISF **EACTDA** te financieren, zodat EACTDA volledig geteste en operationele software-instrumenten zonder licentiekosten en met toegang tot de broncode voor openbareveiligheidsorganisaties van de EU kan leveren.

- De GHN-deskundigen zijn ingenomen met de lopende inspanningen van de Europese Commissie om, in het kader van de financieringsmogelijkheden, het gebruik van het **Europol-instrumentenregister** als centraal knooppunt voor de verspreiding van instrumenten te bevorderen. Zij moedigen het **innovatielab van Europol** aan zijn inspanningen voort te zetten om betrouwbare, veilige, kosteloze, gemakkelijk te installeren en schaalbare onderzoeksinstrumenten ter beschikking te stellen van de rechtshandhavingsinstanties van de EU.

- De GHN-deskundigen vragen om verder na te denken over de **invoering van regelingen voor de evaluatie en – indien relevant – de certificering** van commerciële digitale forensische instrumenten op EU-niveau. Dit kan bijvoorbeeld gebeuren **in het kader van het Europees netwerk van forensische instituten**.

De licenties voor digitale forensische instrumenten zijn duur en soms onbetaalbaar voor sommige rechtshandhavingsinstanties. Door gezamenlijk licenties aan te kopen, die vervolgens tussen autoriteiten in verschillende lidstaten kunnen worden gedeeld, kunnen via onderhandelingen lagere prijzen worden verkregen.

Het *iProcureNet*-project[30], dat in het kader van Horizon Europa wordt gefinancierd, heeft een methode ontwikkeld voor gezamenlijke aanbestedingen op het gebied van beveiliging, en heeft een netwerk van aanbestedende diensten in de lidstaten opgericht. De *Europese innovatiehub voor interne veiligheid* zou, gezien zijn samenstelling en de organisatie van zijn werkzaamheden, bij uitstek geschikt zijn om de lidstaten te helpen hun gemeenschappelijke behoeften in kaart te brengen en te bepalen welke instrumenten het nuttigst zouden zijn, indien er een specifieke digitale forensische werkstroom wordt gecreëerd.

Naast de kostprijs, brengen digitale forensische instrumenten vaak nog andere problemen met zich mee. Gegevens die met deze instrumenten worden opgevraagd, kunnen bijvoorbeeld gestructureerd zijn of gepresenteerd worden in een formaat dat niet compatibel is met de bestaande binnenlandse informatiesystemen die worden gebruikt voor verdere verwerking (bv. gegevensanalyse of -uitwisseling). Daarom moet een reeks gemeenschappelijke eisen van de lidstaten worden geformuleerd met betrekking tot de structuur en het formaat van de gegevens die met behulp van digitale forensische instrumenten worden verkregen. Op basis daarvan zouden de autoriteiten van de lidstaten, bijvoorbeeld in het kader van de reeds genoemde gezamenlijke aanbestedingsprocedures, in dialoog kunnen treden met de aanbieders van digitale forensische instrumenten zodat naar behoren rekening kan worden gehouden met hun eisen.

Kernactie: de GHN-deskundigen benadrukken dat de kosteneffectiviteit van de aankoop van digitale forensische instrumenten moet worden verhoogd

Actoren: lidstaten, Europese Commissie, Europese innovatiehub voor interne veiligheid, Europol	*Tijdschema: vanaf 2025 (gezamenlijke aanbesteding)*	*Begroting: n.v.t.*

- De GHN-deskundigen verzoeken de Europese Commissie:
  - de lidstaten te helpen **bij het in kaart brengen van de digitale forensische instrumenten** die het hardst nodig zijn voor doeltreffende onderzoeken (mogelijk in het kader van de Europese innovatiehub voor interne veiligheid);
  - de **samenwerking tussen operationele eenheden en de contactpunten bij de aanbestedende diensten**, die door iProcureNet zijn samengebracht, te ondersteunen;
  - **proefprojecten** op te zetten voor **de gezamenlijke aankoop van licenties voor digitale forensische instrumenten**.
- De GHN-deskundigen zijn van mening dat **Europol** de lidstaten kan bijstaan bij het bepalen van de **gemeenschappelijke eisen met betrekking tot de structuur en het formaat van gegevens** die met behulp van digitale forensische instrumenten worden verkregen, en op basis daarvan de samenwerking tussen de bevoegde nationale autoriteiten en deskundigen kan bevorderen zodat zij met de producenten en ontwikkelaars van die instrumenten in dialoog kunnen treden om normen af te spreken en naar behoren rekening kan worden gehouden met de eisen van de lidstaten.

[30] https://www.iprocurenet.eu/.

II. Uitwisseling van capaciteiten en delen van gevoelige instrumenten

Momenteel blijft het benutten van kwetsbaarheden om toegang te krijgen tot decryptiesleutels op apparaten de belangrijkste optie voor rechtshandhavingsinstanties om toegang te krijgen tot geëncrypteerde inhoud, aangezien de beschikbaarheid van decryptiecapaciteit (bv. het decryptieplatform van Europol) beperkt is, er geen doeltreffende samenwerking met het bedrijfsleven is en evenmin een specifiek rechtskader om rechtmatige toegang tot informatie op digitale apparaten te waarborgen.

Zelfs als (sommige van) deze voorwaarden enigszins aanwezig zijn, is de kans groot dat criminelen hun toevlucht nemen tot specifieke geëncrypteerde apparaten om informatie of illegale inhoud te verbergen. De rechtshandhavingsinstanties zullen derhalve in de nabije toekomst gevoelige instrumenten[31] en capaciteiten nodig blijven hebben en eventueel moeten delen.

Aanbevelingscluster 2

Om gevoelige instrumenten te delen en de desbetreffende capaciteiten op verantwoorde wijze te beheren, bevelen de deskundigen aan:

1. *na te denken over de invoering van mechanismen om ervoor te zorgen dat gevoelige instrumenten volledig in overeenstemming met de nationale voorschriften kunnen worden gedeeld [aanbeveling 1];*

2. *een proces op te zetten voor de uitwisseling van capaciteiten waarbij mogelijk kwetsbaarheden moeten worden benut, waardoor kennis en middelen kunnen worden gebundeld en tegelijkertijd de eerbiediging van de vertrouwelijkheid en gevoeligheid van de informatie wordt gewaarborgd [aanbeveling 6];*

3. *eventueel een Europese aanpak te onderzoeken voor het beheer en de openbaarmaking van kwetsbaarheden die door rechtshandhavingsinstanties worden verwerkt, op basis van bestaande goede praktijken [aanbeveling 2].*

Via Horizon Europa en het ISF heeft de Europese Commissie projecten (*EXFILES* en *ForRES*[32]) ondersteund die gericht zijn op kwetsbaarheden en de benutting van software en die rechtshandhavers voorzien van instrumenten en protocollen voor snelle en consistente gegevensextractie in overeenstemming met alle toepasselijke wettelijke bepalingen.

---

31 Met “gevoelige instrumenten” worden zowel instrumenten voor digitaal forensisch onderzoek als instrumenten voor tactische interceptie bedoeld.

32 https://forres.eu.

Door gevoelige instrumenten en desbetreffende capaciteiten te delen tussen betrouwbare Europese partners wordt operationele samenwerking vergemakkelijkt, kan onderling kennis worden uitgewisseld en kunnen schaalvoordelen worden gecreëerd, waardoor er minder middelen nodig zijn.

Hoewel het benutten van kwetsbaarheden nog steeds van cruciaal belang kan zijn voor onderzoeken, moet dit uiterst zorgvuldig worden aangepakt, in overeenstemming met het toepasselijke nationale rechtskader, aangezien het negatieve gevolgen voor de beveiligingsmaturiteit van hardware en software met zich meebrengt.

Kernactie: de GHN-deskundigen verzoeken het delen van gevoelige instrumenten en het verantwoorde beheer van desbetreffende capaciteiten te ondersteunen

Actoren: lidstaten, Europese Commissie *Tijdschema: vanaf 2024* *Begroting: n.v.t.*

- De GHN-deskundigen verzoeken de Europese Commissie steun te blijven verlenen aan projecten die gericht zijn op het delen van gevoelige instrumenten (zowel instrumenten voor digitaal forensisch onderzoek als instrumenten voor tactische interceptie) en het bundelen van middelen via relevante financieringsprogramma's. De Commissie zou ook de **oprichting van een transnationaal platform voor het structureren en delen van kennis** kunnen ondersteunen.

- De GHN-deskundigen verzoeken het JRC van de Europese Commissie na te gaan of het haalbaar is een **Europese aanpak** te ontwikkelen **voor het beheer en de openbaarmaking van kwetsbaarheden** die door rechtshandhavingsinstanties worden verwerkt, op basis van bestaande goede praktijken.

III. Collectieve investeringen om vaardigheden te ontwikkelen en deskundigheid op het gebied van digitaal forensisch onderzoek te vergroten

Het betrokken rechtshandhavingspersoneel moet worden opgeleid in het gebruik van onderzoeksinstrumenten en -technieken in het kader van hun onderzoeken, en hun deskundigheid moet worden gecertificeerd. De competenties die zij moeten verwerven en documenteren, moeten hun rol weerspiegelen en ten minste betrekking hebben op generiek (tool-agnostisch) digitaal forensisch onderzoek van mobiele apparaten, bewakingsketengerelateerde onderwerpen en basiskennis over soorten verwerving, analyse, rapportage en presentatie in de rechtbank. Uit de documentatie moet blijken of deze competenties werden verworven door middel van opleiding of op de werkplek.

Aanbevelingscluster 3

Om de ontwikkeling van vaardigheden en deskundigheid op het gebied van digitaal forensisch onderzoek, met inbegrip van decryptie en normalisatie, te ondersteunen, bevelen de deskundigen aan:

1. *het aantal opleidingsmogelijkheden voor deskundigen te verhogen [aanbeveling 7];*
2. *een certificeringsregeling op EU-niveau voor deskundigen op het gebied van digitaal forensisch onderzoek op te zetten om de kwaliteit en uniformiteit van de aangeboden technische opleidingen te waarborgen [aanbeveling 7];*
3. *te investeren om de kloof op het gebied van technische vaardigheden in normalisatie te dichten en het bewustzijn te vergroten door overeenkomsten te sluiten met de academische wereld en andere betrokken instellingen [aanbeveling 8].*

Cepol verzorgt opleidingen over verschillende onderwerpen op dit gebied[33]. De Europese groep voor opleiding in verband met cybercriminaliteit (ECTEG)[34] stelt cursussen op over cybercriminaliteit en digitaal forensisch onderzoek en stelt deze gratis ter beschikking van Cepol en nationale rechtshandhavingsinstanties.

ECTEG heeft *Decrypt* ontwikkeld, een opleidingsmiddel om de capaciteit van de rechtshandhavingsinstanties van de EU-lidstaten op het gebied van legale decryptie te vergroten door middel van geavanceerde strategieën voor rechtmatige verwerking van geëncrypteerd bewijsmateriaal. *Decrypt* kan worden ingezet door Cepol en nationale eenheden, met gebruik van de infrastructuur die het JRC ter beschikking stelt.

---

[33] Opleiding van digitale forensische onderzoekers, forensisch onderzoek van mobiele apparaten, forensisch onderzoek van realtimegegevens en forensisch onderzoek van macOS.

[34] ECTEG is een non-profitorganisatie die dertig rechtshandhavingsinstanties uit twintig Europese landen, internationale organen en de academische wereld samenbrengt. Met steun van het ISF ontwikkelt, bevordert en deelt ECTEG opleidingsmiddelen, -oplossingen en -materiaal. Zie https://www.ecteg.eu/.

Het is evenzeer belangrijk om eerstelijnsfunctionarissen basisvaardigheden op het gebied van digitaal forensisch onderzoek bij te brengen. ECTEG heeft onder meer *eFirst* opgezet ("Educating law enforcement first responders on cyber-essentials" – Basisopleiding cyberkwesties voor eerstelijnsfunctionarissen bij rechtshandhavingsinstanties). *eFirst* is een online opleidingsmodule die politiefunctionarissen in het veld (patrouilles, plaats delict, huiszoeking) of bij wie een slachtoffer een eerste aangifte doet, op eigen tempo kunnen volgen. De opleiding biedt elementaire kennis over cybercriminaliteit en digitaal forensisch onderzoek en kan ook als basis dienen voor fysieke opleidingen in politiescholen.

Door de profielen van deskundigen te certificeren, wordt er gewaarborgd dat elke persoon over de nodige kennis en vaardigheden beschikt. Het stimuleert beroepsbeoefenaars om hun vaardigheden te ontwikkelen en op de hoogte te blijven van de laatste ontwikkelingen in hun vakgebied, en bevordert ook de loopbaanontwikkeling en persoonlijke erkenning. Dit leidt tot hoogwaardiger en nauwkeuriger werk. Bovendien kan een persoonlijke certificering:

- een duidelijke en transparante beschrijving geven van de vaardigheden en competenties van een deskundige op het gebied van digitaal forensisch onderzoek, zodat beroepsbeoefenaars en afdelingshoofden kunnen bepalen wie aan de nodige vereisten moet voldoen om de betrokken taken doeltreffend uit te voeren;

- de ontwikkeling van opleidingen op nationaal, regionaal en EU-niveau vergemakkelijken en de organisatie ervan sturen. Een vergelijkbare politieopleiding in alle EU-lidstaten zorgt ervoor dat alle politiefunctionarissen toegang hebben tot een consistent kennis- en vaardighedenniveau, ongeacht het land waar zij vandaan komen;

- bijdragen tot transparantere gerechtelijke procedures;

- het vertrouwen tussen onderzoekers en andere actoren vergroten, met als gevolg een betere internationale samenwerking tussen nationale rechtshandhavingsinstanties.

Cepol is begonnen met de ontwikkeling van een *sectoraal kwalificatiekader* voor politiewerk, dat gericht is op grensoverschrijdende samenwerking. Dit model kan worden geoperationaliseerd op basis van de werkzaamheden die ECTEG heeft verricht met betrekking tot de certificering van deskundigen op het gebied van digitaal forensisch onderzoek in het kader van haar *Global Cybercrime Certification Project (mondiaal certificeringsproject op het gebied van cybercriminaliteit)*[35].

Zowel ECTEG als EACTDA investeren een deel van hun middelen in de ondersteuning van de daadwerkelijke *deelname van betrokken rechtshandhavers aan normalisatieprocessen*, bijvoorbeeld door hen de nodige vaardigheden te helpen verwerven.

Kernactie: de GHN-deskundigen verzoeken de technische vaardigheden en de certificering van profielen te verbeteren

Actoren: Cepol, ECTEG	*Tijdschema: lopende acties; de certificeringsregeling voor deskundigen op het gebied van digitaal forensisch onderzoek moet uiterlijk in 2026 worden ingevoerd*	*Begroting:*

- De GHN-deskundigen verzoeken Cepol opleidingen te blijven **aanbieden** (met name opleidingen voor opleiders).
- De GHN-deskundigen verzoeken ECTEG door te gaan met het **ontwikkelen, actualiseren en testen** van opleidingen op het gebied van digitaal forensisch onderzoek voor deskundigen en eerstelijnsfunctionarissen, met bijzondere aandacht voor decryptie.
- De GHN-deskundigen zijn ingenomen met de lopende inspanningen van de Commissie (via openbare oproepen tot het indienen van voorstellen in het kader van het ISF) ter ondersteuning van ECTEG, alsook met de **organisatie** van opleidingen op regionaal niveau.
- De GHN verzoekt ECTEG te blijven nagaan of er op EU-niveau een certificeringsregeling voor deskundigen op het gebied van digitaal forensisch onderzoek kan worden ingevoerd, en verzoekt Cepol hieraan zoveel mogelijk bij te dragen, een en ander voortbouwend op hun werkzaamheden inzake respectievelijk **mondiale certificering op het gebied van cybercriminaliteit** en een **sectoraal kwalificatiekader** voor politiewerk.
- De GHN verzoekt ECTEG betrokken beroepsbeoefenaars te blijven helpen bij de verwerving van **competenties en deskundigheid op het gebied van normalisatieprocessen**.

[35] https://www.ecteg.eu/running/gcc/.

IV. Rechtmatige toegang bevorderen

Zonder normen die rechtmatige toegang door ontwerp reguleren, moeten rechtshandhavingsinstanties steeds vaker kwetsbaarheden benutten om toegang te krijgen tot geëncrypteerde informatie op in beslag genomen apparaten. Hoewel deze methode het onderzoek vooruit kan helpen, brengt zij hoge financiële kosten met zich mee. Daarom moet worden nagedacht over mogelijke alternatieven.

Aanbevelingscluster 4

Om mechanismen voor samenwerking met partners uit het bedrijfsleven te ontwikkelen en de mogelijkheid te onderzoeken om bindende normen op te leggen en de wetgeving op het gebied van rechtmatige toegang af te stemmen op de jurisprudentie van het Hof van Justitie van de Europese Unie (HvJ-EU) en het Europees Hof voor de Rechten van de Mens, bevelen de deskundigen aan:

1. *een platform (Sirius of gelijkwaardig) te ontwikkelen voor het delen van instrumenten, beste praktijken en kennis over de wijze waarop producteigenaren, producenten en fabrikanten van hardware toegang tot gegevens moeten verlenen [aanbeveling 11];*

2. *de contactpunten van de rechtshandhavingsinstanties bij de fabrikanten van digitale hardware en software in kaart te brengen [aanbeveling 11];*

3. *een alomvattende inventarisatie van de bestaande wetgeving in de lidstaten te maken en over die wetgeving een EU-handboek op te stellen, teneinde nader te bepalen wat de wettelijke verantwoordelijkheden van fabrikanten van digitale hardware en software zijn met betrekking tot het inwilligen van verzoeken om gegevens van rechtshandhavingsinstanties, rekening houdend met specifieke scenario's en vereisten die ondernemingen dwingen zich toegang te verschaffen tot apparaten [aanbeveling 25];*

4. *een onderzoeksgroep op te richten om de technische haalbaarheid te beoordelen van verplichtingen inzake ingebouwde wettelijke toegang (met inbegrip van de toegang tot geëncrypteerde gegevens) voor digitale apparaten, met behoud van en zonder afbreuk te doen aan de beveiliging van apparaten en de privacy van informatie voor alle gebruikers en zonder de communicatiebeveiliging te verzwakken of te ondermijnen [aanbeveling 26];*

5. *op basis van de bovengenoemde inventarisatie, bindende industriële normen voor apparaten die in de EU in de handel worden gebracht, te ontwikkelen teneinde rechtmatige toegang te integreren en de onderlinge afstemming van de toepasselijke wetgeving te bevorderen [aanbeveling 25].*

De huidige samenwerking tussen de rechtshandhavingsinstanties en het bedrijfsleven is niet bevorderlijk voor concrete resultaten. De samenwerking met het bedrijfsleven moet derhalve worden versterkt om ten behoeve van rechtshandhavingsinstanties te kunnen voorzien in manieren voor rechtmatige toegang tot apparaten en toepassingen. In het geval van videobewakingsopnamen krijgen rechtshandhavingsinstanties bijvoorbeeld steeds meer te maken met geëncrypteerde bestanden die niet automatisch met software kunnen worden geanalyseerd, met name wanneer het gaat om grote hoeveelheden video-opnamen.

In theorie kunnen rechtshandhavingsinstanties ondersteuning vragen aan fabrikanten van apparaten, die de broncode van hun software kunnen verstrekken om de toegang tot niet-gecodeerde inhoudelijke gegevens te vergemakkelijken, of die de technische documentatie kunnen overleggen van apparatuur die in strafrechtelijke onderzoeken wordt aangetroffen.

Europol is bij uitstek geschikt om beste praktijken te verzamelen (zoals de oprichting van contactpunten voor rechtshandhavingsinstanties) en kennis te vergaren over de wijze waarop producteigenaren, producenten en hardwarefabrikanten de toegang kunnen vergemakkelijken en deze via Sirius (of een gelijkwaardig platform) aan alle rechtshandhavingsinstanties ter beschikking kunnen stellen.

Tegelijkertijd moeten transparantere oplossingen worden overwogen die toegang tot niet-gecodeerde gegevens op in beslag genomen apparaten mogelijk maken, zodat onderzoeken doeltreffender verlopen en tegelijkertijd een gelijk speelveld tussen alle spelers in de sector tot stand wordt gebracht, een en ander onder vrijwaring van de cyberbeveiliging en de privacy.

Op basis van een gedetailleerde analyse van de rechtshandhavingsvereisten voor rechtmatige toegang dringen de deskundigen er bij de Europese Commissie op aan een *technologieroutekaart*[36] op te stellen waarin de acties van deskundigen op het gebied van technologie, cyberbeveiliging, privacy, normalisatie en beveiliging worden gebundeld en waarmee een adequate coördinatie wordt gewaarborgd.

Een belangrijke actie in het kader van deze technologieroutekaart zou erin bestaan de *technische haalbaarheid van verplichtingen inzake ingebouwde rechtmatige toegang* te beoordelen (onder meer voor de toegang tot geëncrypteerde gegevens en geëncrypteerde CCTV-opnamen) voor digitale bestanden en apparaten[37], waarbij wordt voorzien in solide waarborgen voor de cyberbeveiliging en de communicatiebeveiliging niet wordt verzwakt of ondermijnd. Bij deze beoordeling zouden alle belanghebbenden worden betrokken.

---

[36] In het verslag wordt meermaals en in verschillende hoofdstukken verwezen naar een unieke "technologieroutekaart".

[37] Zie "Moving the Encryption Policy Conversation Forward" – Carnegie Endowment for International Peace – https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Indien uit dergelijke beoordeling blijkt dat verplichtingen inzake ingebouwde rechtmatige toegang overeenkomstig de bovenstaande voorwaarden beschikbaar of haalbaar zijn, moet in de technologieroutekaart ook het proces voor een duurzame *langetermijnsamenwerking met normalisatie-instellingen* worden omschreven. De deelname van rechtshandhavingsinstanties aan dit normalisatieproces kan worden gecoördineerd door Europol, met de steun van EACTDA.

Op basis van een inventarisatie van de bestaande rechtskaders van de lidstaten waarin de verantwoordelijkheden van fabrikanten van digitale hardware en software met betrekking tot het inwilligen van verzoeken om gegevens van rechtshandhavingsinstanties worden vastgelegd, kan worden beoordeeld of er *wetgeving of richtsnoeren en aanbevelingen* [waarbij de toepasselijke wetgeving wordt geharmoniseerd] nodig zijn.

Kernactie: de GHN-deskundigen pleiten voor meer samenwerking met het bedrijfsleven, een betere verwijzing naar toepasselijke normen in toekomstige EU-initiatieven en de onderlinge afstemming van de wetgeving op het gebied van rechtmatige toegang in overeenstemming met de jurisprudentie van het HvJ-EU en het Europees Hof voor de Rechten van de Mens.

Actoren: Europol; Europese Commissie *Tijdschema: vanaf 2025* *Begroting: n.v.t.*

- De GHN-deskundigen verzoeken de **Europese Commissie** een specifieke **technologieroutekaart** te ontwikkelen om de mogelijkheden voor rechtmatige toegang tot digitale apparaten te onderzoeken.
- De GHN-deskundigen verzoeken **Europol** beste praktijken te verzamelen en kennis te vergaren over de wijze waarop producteigenaren, producenten en hardwarefabrikanten de toegang kunnen vergemakkelijken en deze via **Sirius** (of een gelijkwaardig platform) aan alle rechtshandhavingsinstanties ter beschikking kunnen stellen.

Hoofdstuk II: gegevensbewaring

WAAR GAAT HET OM?

Terwijl vroeger vooral fysiek bewijsmateriaal werd verzameld, slaan aanbieders van communicatiediensten tegenwoordig een enorme hoeveelheid potentieel bewijsmateriaal op in de vorm van metagegevens. Hoewel er in de context van een strafrechtelijk onderzoek ook behoefte is aan andere soorten bewijsmateriaal, zijn digitale gegevens in bijna alle onderzoeken, ongeacht of deze betrekking hebben op strafbare feiten in de fysieke of in de digitale wereld, van cruciaal belang om met name de identiteit vast te stellen van verdachten of personen van belang die mogelijk over relevante informatie beschikken. Vooral in een digitale omgeving kan een verdachte vaak alleen worden geïdentificeerd aan de hand van communicatiemetagegevens (met name IP-adressen en poortnummers)[38].

In het digitale tijdperk kunnen rechtshandhavingsinstanties maar een onderzoek naar strafbare feiten voeren indien digitaal bewijsmateriaal beschikbaar wordt gesteld in een leesbaar formaat en, waar nodig, toegankelijk is, met passende waarborgen op het gebied van strafprocedures, procedurele rechten, privacy en de bescherming van persoonsgegevens. Gegevens kunnen worden bewaard voor zakelijke doeleinden (zoals facturering) of voor rechtshandhavingsdoeleinden. Gegevensbewaring kan ertoe bijdragen dat gegevens beschikbaar zijn voor de bevoegde autoriteiten in het kader van een strafrechtelijk onderzoek of een vervolging. Door aanbieders bewaarde gegevens kunnen van cruciaal belang zijn om criminaliteit doeltreffend te bestrijden. Alleen indien dergelijke gegevens worden bewaard, kunnen rechtshandhavingsinstanties er later toegang toe krijgen en onderzoek verrichten[39]. Tegelijkertijd wordt in het beginsel van minimale gegevensverwerking dat is vastgelegd in de e-privacyrichtlijn[40] en de algemene verordening gegevensbescherming (AVG)[41] bepaald dat aanbieders verkeersgegevens alleen mogen opslaan (of anderszins verwerken) zolang dat nodig is voor de communicatie zelf, voor facturering of, in specifieke situaties, voor de marketing van elektronischecommunicatiediensten. Elke andere vorm van opslag moet worden geregeld door middel van een juridisch kader dat voldoet aan artikel 15 van de e-privacyrichtlijn. Deze regeling weerspiegelt de noodzaak om een evenwicht te vinden tussen enerzijds de grondrechten van privacy en gegevensbescherming en anderzijds het beoogde effect van rechtshandhavingsmaatregelen.

---

38 Deskundigen hebben zich gebogen over verschillende gevallen waarin digitale gegevens relevant waren voor een onderzoek en hebben gekeken naar het aantal verzoeken om gegevens. Volgens een van de deskundigen is in de afgelopen vijf jaar bij alle onderzoeken naar terrorisme of georganiseerde criminaliteit gebruikgemaakt van gegevens die bij aanbieders zijn opgevraagd. In 2023 werden in één lidstaat bij exploitanten meer dan 1 300 000 nummers opgevraagd voor identificatie in strafprocedures. Bijna alle aanvragen werden nadien door de rechtbank bekrachtigd.

39 Voor deze nota wordt onder “toegang tot gegevens” verstaan: toegang die per geval wordt verleend aan rechtshandhavingsinstanties, indien nodig met voorafgaande toestemming van de rechter, met het oog op een strafrechtelijk onderzoek.

40 Artikel 6 van Richtlijn 2002/58/EG.

41 Artikel 5, lid 1, punt c), van Verordening (EU) 2016/679.

Momenteel bestaat er geen EU-wetgeving inzake gegevensbewaring. Het HvJ-EU heeft de gegevensbewaringsrichtlijn van de EU[42] in 2014 nietig verklaard, waarbij het heeft gewezen op de aanzienlijke inmenging in de grondrechten van privacy en gegevensbescherming die inherent is aan de [algemene en willekeurige] opslag voor rechtshandhavingsdoeleinden van oorspronkelijk door dienstverleners verzamelde gegevens[43]. Dit heeft aanleiding gegeven tot wijzigingen in de nationale rechtskaders, die nu aanzienlijk onderling verschillen binnen de EU[44]: terwijl sommige lidstaten aanbieders van communicatiediensten nog steeds verplichten om bepaalde categorieën gegevens te bewaren voor rechtshandhavingsdoeleinden, hebben andere lidstaten wijzigingen doorgevoerd om te voldoen aan het in de jurisprudentie voorgestelde criterium van gerichte bewaring van verkeersgegevens.[45] Weer andere lidstaten hebben, mede als gevolg van latere uitspraken van nationale rechtbanken, geen specifieke regels voor het bewaren van gegevens voor rechtshandhavingsdoeleinden, maar verlaten zich uitsluitend op gegevens die door ondernemingen worden bewaard voor zakelijke doeleinden. De voorwaarden voor toegang tot dergelijke gegevens hangen af van het vigerende nationale rechtskader en het soort gegevens (abonneegegevens, verkeersgegevens of inhoudelijke gegevens). Door dit gebrek aan coherente en geharmoniseerde verplichtingen inzake gegevensbewaring in de EU bestaan er in de lidstaten uiteenlopende voorschriften voor het bewaren van verschillende soorten metagegevens door dienstverleners (en voor de bewaringsduur).

---

42 Richtlijn 2006/24/EG. Volgens de richtlijn moesten de EU-lidstaten maatregelen nemen om ervoor te zorgen dat aanbieders van elektronischecommunicatiediensten en -netwerken verkeers- en locatiegegevens en de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren, bewaren voor een periode van zes maanden tot twee jaar, zodat de bevoegde autoriteiten er toegang toe zouden krijgen voor het onderzoeken, opsporen en vervolgen van ernstige strafbare feiten zoals gedefinieerd in de nationale wetgeving.

43 Voor een overzicht van de relevante jurisprudentie, zie: The future of national data retention obligations – How to apply Digital Rights Ireland at national level? – European Law Blog, V. Franssen; Recalibrating Data Retention in the EU - eucrim; verslag van Eurojust/EJCN 2024 "The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU"; justitiële monitor cybercriminaliteit – uitgave 6; justitiële monitor cybercriminaliteit – uitgave 9.

44 De lidstaten hebben op verschillende manieren gereageerd op de nietigverklaring van de gegevensbewaringsrichtlijn, met nationale maatregelen die aanleiding gaven tot verder uiteenlopende nationale systemen voor gegevensbewaring. Volgens het verslag over gegevensbewaring van Eurojust/EJCN van 2024 hebben in de periode 2018-2022 twaalf landen hun wetgeving gewijzigd. Volgens de respondenten waren deze wijzigingen een rechtstreeks gevolg van zaak C-746/18 (Prokuratuur) en de gevoegde zaken C-511/18, C-512/18 en C-520/18 (La Quadrature du Net e.a.). 23 van de 27 lidstaten beschikken over regels inzake gegevensbewaring; 7 lidstaten hebben al regels voor gerichte gegevensbewaring ingevoerd. Zie voor een overzicht de volgende studie van de Commissie: Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, blz. 39.

45 Het Hof heeft het begrip gerichte bewaring van verkeers- en locatiegegevens in verschillende arresten ontwikkeld en heeft daarbij geoordeeld dat de bewaring van gegevens verenigbaar kan zijn met het EU-recht indien deze is opgezet rond en voor specifieke doelstellingen. Hoge rechtbanken in de lidstaten die geprobeerd hebben de door het Hof voorgestelde criteria voor het bepalen van die doelstellingen in de praktijk toe te passen, hebben daarbij echter moeilijkheden en problemen ondervonden.

In de lidstaten zonder verplichte gegevensbewaring is het moeilijk of soms zelfs onmogelijk om een verdachte in een strafrechtelijk onderzoek of een persoon die mogelijk over relevante informatie beschikt in een dergelijk onderzoek ("persoon van belang"), te identificeren[46]. De nieuwe regels inzake elektronisch bewijsmateriaal zouden, zodra zij van kracht zijn, ook een grotere toegevoegde waarde hebben indien zij worden aangevuld met een verplichte gegevensbewaring. Anders zijn er immers geen garanties omtrent de beschikbaarheid van de informatie waarop een Europees bewarings- of verstrekkingsbevel betrekking heeft (verkeersgegevens, gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker, en abonneegegevens).

De huidige omstandigheden hebben gevolgen voor zowel **rechtshandhavingsinstanties** als **aanbieders van communicatiediensten**, maar vooral ook **voor burgers en slachtoffers**, van wie het recht op toegang tot de rechter niet gewaarborgd is als bij de start van het onderzoek blijkt dat gegevens reeds zijn gewist of niet zijn bewaard[47].

I. Problemen binnen de jurisdictie van individuele lidstaten

In lidstaten **zonder specifieke verplichtingen** voor het bewaren van gegevens voor rechtshandhavingsdoeleinden, worden de onderzoeken verricht op basis van de gegevens die ondernemingen opslaan voor zakelijke en commerciële doeleinden, naast ander beschikbaar bewijsmateriaal. Commerciële gegevens zijn onderworpen aan het interne beleid van de aanbieders, waarbij ondernemingen verschillende perioden hanteren voor het opslaan van verkeersgegevens (bijvoorbeeld ongeveer zes maanden), terwijl locatiegegevens, die doorgaans geen zakelijk belang dienen, vaak minder lang worden bewaard. Vaak slaan kleine ondernemingen geen abonnee- of communicatiemetagegevens op of bewaren ze deze voor een zeer korte tijd. Daardoor zijn onderzoeken vaak een race tegen de klok, aangezien de onderzoekers moeten nagaan wie de aanbieder van de gegevens is en overeenkomstig de toepasselijke regels een verzoek moeten indienen voordat de gegevens worden gewist, wat soms een kwestie van dagen of uren is. In sommige gevallen verstrekken ondernemingen geen informatie over de specifieke gegevens die zij verwerken en bewaren, waardoor het voor de bevoegde autoriteiten moeilijk is om een gericht verzoek om gegevens in te dienen. Bij sommige hostingdiensten kunnen gebruikers fictieve gegevens gebruiken om serverruimte te huren, wat betekent dat zelfs indien gebruikersgegevens worden opgeslagen, deze niet betrouwbaar zijn[48].

---

46 Zie het voorbeeld dat wordt gegeven in het achtergronddocument "Operational challenges faced by law enforcement related to access to data – Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement", blz. 4.

47 In de context van de gevolgen voor burgers en slachtoffers, zie Dwyer/Commissioner of An Garda Siochána – [2020] IESC 4 (24/02/2020), met name punt 9.

48 https://en.wikipedia.org/wiki/Bulletproof_hosting.

De meeste lidstaten **beschikken over wetgeving inzake gegevensbewaring**. Zoals hierboven beschreven, is de nationale wetgeving is sommige gevallen echter gewijzigd naar aanleiding van arresten van het HvJ-EU die voortvloeiden uit de nietigverklaring van de gegevensbewaringsrichtlijn. Daardoor is een gemengd beeld ontstaan, waarbij de lidstaten verschillend hebben gereageerd op uitspraken. In sommige lidstaten zijn inspanningen geleverd om een gerichte vorm van bewaring in te voeren, zoals voorgesteld door het HvJ-EU als een mogelijke stap voorwaarts op het gebied van gegevensbewaring. Volgens de GHN-deskundigen hebben dergelijke criteria echter geleid tot juridische en technische problemen op het gebied van haalbaarheid[49], terwijl de aanbieders zich kritisch hebben uitgelaten over de kosten in verband met de technische uitvoering van gerichte bewaring en, meer in het algemeen, van de frequent wijzigende wetgeving. Een ander belangrijk juridisch probleem op nationaal niveau is dat de nationale wetgeving in de meeste gevallen geen betrekking heeft op OTT-diensten. Het specifieke geval van OTT-diensten komt uitgebreider aan bod in punt 1.3.

II. Grensoverschrijdende kwesties in de EU

Problemen in verband met gegevensbewaring doen zich ook voor bij grensoverschrijdende verzoeken, d.w.z. wanneer een bevoegde autoriteit gegevens opvraagt bij een aanbieder die in een andere lidstaat is gevestigd. Bij een grensoverschrijdend verzoek kan het gebeuren dat de autoriteiten van het ontvangende land geen gevolg kunnen geven aan het verzoek van het andere land (wegens het ontbreken van gegevens of desbetreffende wetgeving).

Het ontbreken van EU-wijde geharmoniseerde verplichtingen inzake het bewaren van metagegevens belemmert de rechtshandhaving in lidstaten **die gegevens nodig hebben** van een in een andere lidstaat gevestigde aanbieder. Hoewel er regelingen voor gegevensbewaring bestaan op nationaal niveau, ontbreekt een coherente benadering van bewaartermijnen, die aanzienlijk verschillen van lidstaat tot lidstaat[50].

---

[49] Hoewel het HvJ-EU de **gerichte bewaring** van verkeersgegevens toelicht aan de hand van richtsnoeren en voorbeelden, is de jurisprudentie slechts richtinggevend en bevat zij geen nauwkeurig overzicht van de mogelijke beperkingen op de bewaring voor alle gegevenscategorieën. Als gevolg daarvan zijn de afgelopen jaren bij het Hof verschillende zaken aanhangig gemaakt tegen regels inzake gegevensbewaring en kunnen de lidstaten geen rechtszekerheid waarborgen.

[50] Afhankelijk van de gegevens en de aard van het strafbare feit worden metagegevens bewaard tussen 6 en 72 maanden. In het verslag over gegevensbewaring van Eurojust/EJCN van 2024 gaven respondenten aan dat er minder gegevens beschikbaar waren als gevolg van het niet bewaren van gegevens, beperkingen op de categorieën gegevens die kunnen worden bewaard, en korte(re) bewaartermijnen. Bijgevolg heeft het ontbreken van gegevens ook gevolgen voor het vermogen van de autoriteiten om Europese onderzoeksbevelen en verzoeken om wederzijdse rechtshulp uit te voeren.

Evenmin bestaat er op EU-niveau een geharmoniseerde aanpak inzake de **definitie van de gegevens** die moeten worden bewaard[51]. De nationale wetgeving kan dienstverleners verplichten om verschillende categorieën gegevens te bewaren voor verschillende doeleinden (belastingen, audits, rechtshandhaving). De regels zijn in dit verband ook niet altijd even gedetailleerd: sommige wetgevingen bevatten gedetailleerde lijsten van niet-inhoudelijke gegevens die moeten worden bewaard, terwijl andere voorzien in ruimere definities van niet-inhoudelijke gegevens[52]. Voorts bewaren aanbieders, afhankelijk van de dienst die zij aanbieden en van hun zakelijke en commerciële behoeften, de verschillende soorten gegevens gedurende een verschillende periode. Dit geeft een zeer gemengd beeld, met niet alleen aanzienlijke verschillen tussen de lidstaten, maar ook tussen de diensten onderling.

Dergelijke verschillen zijn tevens relevant omdat ook de toegang tot bewaarde gegevens per lidstaat verschilt: in sommige lidstaten is rechterlijke toestemming nodig om toegang te krijgen tot bepaalde soorten metagegevens, terwijl dat in andere lidstaten niet het geval is. Dienstverleners melden dat rechtsonzekerheid over de regels met betrekking tot de openbaarmaking van gegevens een van de redenen is waarom aan verzoeken van rechtshandhavingsinstanties laattijdig of geen gevolg wordt gegeven.

---

51 Zoals blijkt uit de studie van de Commissie over gegevensbewaring, blz. 48: “Bepaalde soorten informatie worden in alle lidstaten altijd als abonnee- of verkeersgegevens beschouwd, maar er is geen consensus over de classificering van de volgende gegevenspunten: IP-adressen, simkaartnummers, apparaatidentificatienummers (bv. IMSI, IMEI) en poortnummers voor dynamische IP-adressen. In sommige lidstaten (EE, FR, IE) worden deze gegevenspunten geclassificeerd als abonneegegevens, in andere lidstaten (DE, ES, IT, PL, SI) als verkeersgegevens” (eigen vertaling).

52 Zie de studie van de Commissie over gegevensbewaring, bijlage III, voor een overzicht van de per lidstaat bewaarde gegevens.

De bevoegde autoriteiten moeten voldoen aan de nationale regelgeving die van toepassing is op de aanbieder die de gevraagde gegevens bewaart, maar ook aan de specifieke eisen van de aanbieders zelf. Zoals gerapporteerd in het Sirius-jaarverslag van 2022[53], kunnen aanbieders verlangen dat gebruik wordt gemaakt van speciale portalen, of dat verzoeken worden ingediend via een specifieke template of in een specifieke taal. Zij kunnen ook verlangen dat informatie wordt gegeven over de aard van de zaak, dat duidelijk wordt verwezen naar de nationale rechtsgrond voor het verzoek, of dat de periode waarvoor gegevens worden opgevraagd, nauw wordt omschreven. Hoewel sommige van deze kwesties uiterlijk in 2026 zullen zijn opgelost met de uitvoering van het pakket elektronisch bewijsmateriaal, benadrukten de GHN-deskundigen de noodzaak van samenhang tussen deze regels enerzijds en een eventueel geharmoniseerd kader voor gegevensbewaring anderzijds. Het Europees Instituut voor telecommunicatienormen (ETSI) heeft weliswaar normen ontwikkeld voor het formaat van verzoeken om metagegevens van nummergebaseerde interpersoonlijke communicatiediensten (traditionele telecommunicatie), maar de aanbieders passen die niet consequent toe in de lidstaten. De normen voor datatransmissie van aanbieders van OTT-diensten[54] aan rechtshandhavingsinstanties zijn een werk in uitvoering en worden niet volledig toegepast. Bovendien kunnen dienstverleners zelf beslissen in welke vorm zij gebruikersgegevens verzamelen en opslaan, waardoor beroepsbeoefenaars ruwe gegevens in zeer verschillende vormen ontvangen. Dit brengt een aanzienlijke last met zich mee voor rechtshandhavingsinstanties, die baat zouden hebben bij gestroomlijnde processen, **communicatiesystemen en formaten** voor het indienen van verzoeken en voor het verzenden en ontvangen van antwoorden op verzoeken en van gegevens. Tevens zouden gestandaardiseerde communicatiesystemen en -formaten ervoor zorgen dat ondernemingen minder kosten hebben voor het verwerken van verzoeken.

Zodra rechtshandhavingsinstanties rechtmatige toegang tot gegevens hebben verkregen, moeten zij die kunnen benutten. De gegevens moeten dus **leesbaar** zijn. Steeds vaker worden echter diensten aangeboden die eind-tot-eindencryptie van verkeersgegevens mogelijk maken. Als rechtshandhavings- en rechterlijke instanties dergelijke gegevens opvragen, ontvangen ze die vaak in geëncrypteerde vorm.

---

[53] sirius-eu-digital-evidence-situation-report-2022, blz. 14.

[54] In dit verslag verwijst de term “over-the-topcommunicatiediensten” (“OTT-communicatiediensten”) naar toepassingen en diensten die communicatie- en mediadiensten (zoals berichtenverkeer, spraakoproepen en videogesprekken) via internet aanbieden zonder tussenkomst van of controle door traditionele aanbieders van telecommunicatiediensten (telecomproviders). Gangbare voorbeelden van OTT-communicatiediensten zijn berichtenapps zoals WhatsApp, Telegram en Facebook Messenger, spraak- en videodiensten zoals Skype, Zoom, Google Meet en Viber, en socialemediaplatforms zoals Instagram en Snapchat (uitwisselen van berichten en delen van media).

Tot slot is een ander mogelijk gevolg van deze status quo dat **bewijsmateriaal** van rechtshandhavingsinstanties voor de rechter wordt **aangevochten**[55]. Het HvJ-EU heeft verduidelijkt dat de aanvaarding van door middel van gegevensbewaring verkregen bewijsmateriaal een zaak is van het nationale recht[56], waarbij het gelijkwaardigheids- en het doeltreffendheidsbeginsel in acht moeten worden genomen[57]. Verschillen tussen nationale regelingen voor gegevensbewaring kunnen dus gevolgen hebben voor de toelaatbaarheid van bewijsmateriaal in grensoverschrijdende procedures[58].

---

55 Zie het hoofdstuk "Collection and admissibility of evidence" [Verzameling en toelaatbaarheid van bewijsmateriaal] in het verslag over gegevensbewaring van Eurojust/EJCN van 2024).

56 Arrest van het HvJ-EU van 6 oktober 2020, La Quadrature du Net e.a., zaak C-511/18, ECLI:EU:C:2020:791, punten 222-228; arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., zaak C-140/20, ECLI:EU:C:2022:258, punt 127.

57 Ibid., punt 223: "… op voorwaarde [...] dat die regels niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel)."

58 De ontvankelijkheid van niet-inhoudelijke gegevens als bewijsmateriaal is in verschillende rechtszaken betwist. Een samenvatting is terug te vinden in de studie van de Commissie over gegevensbewaring, blz. 41.

III. Kwesties in verband met OTT- en andere aanbieders

De bovenstaande kwesties hebben betrekking op alle aanbieders van elektronischecommunicatiediensten. OTT-aanbieders stellen de rechtshandhavingsinstanties echter voor extra uitdagingen als het gaat om rechtmatige toegang tot gegevens. Zowel op nationaal als op EU-niveau voelen OTT-aanbieders zich vaak niet gebonden aan dezelfde verplichtingen als traditionele aanbieders van communicatiediensten. OTT-aanbieders vallen onder het toepassingsgebied van het EECC, maar het feit dat zij vaak buiten de EU zijn gevestigd en het ontbreken van vergunningsstelsels (d.w.z. dat zij mogelijk slechts een algemene vergunning nodig hebben) en van sancties leidt tot onzekerheid over hun verplichting om gegevens, waaronder specifieke soorten gegevens, te bewaren. Het zorgt ook voor handhavingsproblemen. Bovendien bewaren traditionele aanbieders van communicatiediensten in de meeste gevallen bepaalde voor zakelijke doeleinden bestemde gegevens waarmee gebruikers kunnen worden geïdentificeerd (zoals IP-nummers met poortnummer en tijdsbestek). Dit is echter niet het geval voor **aanbieders van OTT-diensten**, die alleen de niet-inhoudelijke gegevens bewaren die zij nodig hebben voor commerciële doeleinden, en soms maar voor een korte periode[59]. OTT-aanbieders bewaren geen niet-inhoudelijke gegevens die gelinkt zijn aan een dynamisch IP-adres (poortnummer en tijdsbestek). Daardoor kan het moeilijk of zelfs onmogelijk zijn om metagegevens te verkrijgen van communicatie via systemen als WhatsApp of Telegram, die steeds vaker worden gebruikt. Zoals reeds vermeld, variëren de soorten bewaarde gegevens ook naargelang de aangeboden dienst. Terwijl de aanbieders in sommige gevallen richtlijnen uitvaardigen met een beschrijving van de soorten gegevens die zij bewaren[60], maken OTT-aanbieders deze informatie in andere gevallen niet bekend. In combinatie met het gebrek aan **transparantieverplichtingen** met betrekking tot de soorten gegevens die aanbieders voor zakelijke doeleinden genereren, verwerken en opslaan, leidt dit tot frequente problemen voor rechtshandhavingsinstanties wanneer zij proberen na te gaan of gegevens zijn bewaard, wie in het bezit is van welke gegevens en welke soorten datasets kunnen worden opgevraagd, en uiteindelijk wanneer zij een verzoek sturen naar een aanbieder.

---

59 Dit geldt met name voor kleine aanbieders. Volgens de studie van de Commissie over gegevensbewaring, blz. 103, worden IP-adressen gemiddeld dertig dagen bewaard.

60 Zie bijvoorbeeld law-enforcement-guidelines-outside-us.pdf (apple.com).

Tegelijkertijd draagt het toenemende aantal verzoeken aan aanbieders[61], in combinatie met de noodzaak om zeer grote datasets te verwerken, ertoe bij dat soms te laat of afwijzend op verzoeken wordt gereageerd[62]. Dit houdt niet alleen verband met de keuze van aanbieders voor een specifiek bedrijfsmodel, maar is ook te wijten aan het **beperkte aantal mechanismen voor samenwerking** tussen rechtshandhavings- en rechterlijke instanties enerzijds en particuliere ondernemingen anderzijds.

Tot slot vallen een aantal opkomende technologieën en andere digitale spelers (zoals autofabrikanten en AI-systemen op basis van een large language model (LLM)) niet onder de EECC-definitie van aanbieder van communicatiediensten, maar genereren en verwerken zij wel een aantal communicatiemetagegevens die informatie kunnen verschaffen over criminele activiteiten. Hoewel deze diensten steeds meer gegevens verwerken, zijn zij momenteel niet gebonden aan verplichtingen inzake gegevensbewaring.

MOGELIJKE OPLOSSINGEN

I. Versterkte samenwerking tussen aanbieders van communicatiediensten en beroepsbeoefenaars

In een context waarin het verzamelen van digitaal bewijsmateriaal wordt belemmerd door een gebrek aan geharmoniseerde regels, moeten rechtshandhavingsinstanties die een onderzoek verrichten, zich vaak verlaten op **vrijwillige samenwerking** met dienstverleners. Hoewel deze oplossing het onderzoek in bepaalde belangrijke zaken heeft vooruitgeholpen[63], biedt ze geen rechtszekerheid en is ze niet altijd haalbaar. Vrijwillige medewerking is immers afhankelijk van het type en de omvang van de dienstverlener, waarbij kleine dienstverleners gegevens vaak voor een zeer korte periode bewaren in vergelijking met grotere dienstverleners, of niet over de middelen beschikken om in te gaan op verzoeken van rechtshandhavingsinstanties[64].

---

61 Volgens het Sirius-jaarverslag 2023 neemt het aantal verzoeken om gegevens aan dienstverleners elk jaar gestaag toe (zie blz. 66 e.v.).

62 Het Sirius-jaarverslag 2023 (voetnoot 61) bevat een overzicht van de belangrijkste oorzaken van laattijdige/afwijzende reacties op verzoeken om elektronisch bewijsmateriaal (zie blz. 68 e.v.).

63 Zie voorbeelden in het Sirius-jaarverslag 2023 (voetnoot 61), blz. 19.

64 In het Sirius-jaarverslag 2023 (voetnoot 61), blz. 79, staat dat het grote aantal verzoeken in het kader van vrijwillige samenwerking een uitdaging vormt voor dienstverleners, en wordt aanbevolen dat zij deelnemen aan internationale Sirius-evenementen, zodat "kleinere onlinedienstverleners kunnen profiteren van de deskundigheid van het Sirius-project op het gebied van samenwerking met de autoriteiten om hun inzicht in de materie te vergroten, hun beleid voor het beantwoorden van verzoeken van autoriteiten te structureren, en ervoor te zorgen dat zij voorbereid zijn op toekomstige ontwikkelingen op wetgevingsgebied" (eigen vertaling).

Partnerschappen en samenwerking met het bedrijfsleven moeten worden geschraagd door een **duidelijk rechtskader**, als essentieel onderdeel van elke haalbare oplossing voor problemen die rechtshandhavings- en rechterlijke instanties ondervinden op het gebied van rechtmatige toegang tot digitaal bewijsmateriaal. Beide partijen moeten niet alleen aan hun respectieve wettelijke verplichtingen voldoen, er moet ook sprake zijn van een permanente vertrouwensrelatie tussen rechtshandhavingsinstanties en aanbieders, zodat zij elkaars behoeften begrijpen en samen werkbare oplossingen kunnen vinden. Stabiele **mechanismen voor samenwerking** met de particuliere sector zijn niet alleen nodig om **meer transparantie te bieden** over de door aanbieders gegenereerde en opgeslagen gegevens en de bewaartermijn ervan, maar ook om te zorgen voor een **geharmoniseerde categorisering van de gegevens** die moeten worden bewaard en kunnen worden opgevraagd, het ontwerpen van **gestandaardiseerde formaten** voor het opvragen van gegevens, en het opzetten van **veilige kanalen** voor rechtstreekse uitwisseling tussen bevoegde autoriteiten en dienstverleners.

Er kunnen verschillende mogelijkheden voor een dergelijke samenwerking worden onderzocht, waarvan sommige bindend zijn (harde wetgeving) en andere bestaan uit zachte wetgeving. Sommige van de in dit deel genoemde oplossingen moeten worden beoordeeld in het kader van de in deel II bedoelde effectbeoordeling en vervolgens bij wet worden vastgesteld.

Aanbevelingscluster 5

Om ervoor te zorgen dat de bevoegde autoriteiten kunnen nagaan tot welke gegevenshouders zij zich moeten richten om relevante gegevens te verkrijgen, dat dienstverleners verzoeken om gegevens ontvangen in een gestandaardiseerd formaat, en dat grensoverschrijdende samenwerking niet wordt belemmerd door wetsconflicten, bevelen de deskundigen het volgende aan:

1. *samenwerking tussen rechtshandhavingsinstanties en dienstverleners tot stand brengen en intensiveren ter ondersteuning van informatie-uitwisseling, capaciteitsopbouw en opleiding en om ervoor te zorgen dat de beginselen en voorwaarden voor samenwerking worden vastgesteld [aanbeveling 13], bijvoorbeeld door een coördinatiecentrum op te richten dat de bevoegde autoriteiten in staat stelt de relevante dienstverleners in kaart te brengen en rechtmatige verzoeken gerichter te formuleren [aanbeveling 18]. Dit kan worden bereikt door:*

    a. *voort te bouwen op bestaande structuren op EU-niveau, zoals Sirius, het Europees justitieel netwerk (EJN) / Europees justitieel netwerk cybercriminaliteit (EJCN) en het EU-Internetforum;*

    b. *memoranda van overeenstemming te sluiten, waarbij wordt geprofiteerd van beste praktijken die in bepaalde lidstaten op nationaal niveau worden gehanteerd [aanbeveling 14];*

2. *transparantieregels bevorderen voor aanbieders van elektronischecommunicatiediensten en andere communicatiediensten met betrekking tot de gegevens die zij verwerken, genereren of opslaan in de bedrijfsuitoefening, en inzake het informeren van rechtshandhavingsinstanties over welke gegevens beschikbaar zijn, rekening houdend met de beperkingen die voortvloeien uit de vertrouwelijkheid van onderzoeken, door middel van samenwerkingsovereenkomsten met dienstverleners of, indien nodig, door bindende voorschriften vast te stellen [aanbeveling 17, aanbeveling 16];*

3. *gestroomlijnde processen en formaten ontwikkelen op basis van overeengekomen normen, zodat het indienen van verzoeken bij aanbieders en het ontvangen van antwoorden gestructureerd verloopt [aanbeveling 15], en de aanwijzing binnen platforms bevorderen van centrale contactpunten voor de behandeling van verzoeken van en contacten met de bevoegde autoriteiten [aanbeveling 36];*

4. *mechanismen opzetten om ervoor te zorgen dat grensoverschrijdende verzoeken op efficiënte wijze aan dienstverleners worden gericht en dat potentiële conflicten worden vermeden, waarbij inspiratie wordt geput uit mechanismen voor elektronisch bewijsmateriaal en ervoor wordt gezorgd dat die mechanismen consistent zijn met de regels van de verordening elektronisch bewijsmateriaal [aanbeveling 19].*

Dankzij reeds bestaande EU-structuren kunnen de betrokken actoren zich vertrouwd maken met instrumenten en beste praktijken. Door rechtshandhavingsinstanties, rechterlijke instanties en dienstverleners samen te brengen, kan het Sirius-project zorgen voor een eenvoudigere uitwisseling van kennis en instrumenten met betrekking tot verzoeken om gebruikersgegevens aan aanbieders[65], en kan het dienen als platform voor rechtstreekse contacten tussen verzoekende autoriteiten en aanbieders, met name dankzij het bestaande Sirius-netwerk van centrale contactpunten[66]. Sirius zou kunnen dienen als **centraal register** voor rechtsinstrumenten, jurisprudentie, formaten enzovoort, zoals reeds het geval is in het kader van de grensoverschrijdende uitwisseling van elektronisch bewijsmateriaal[67].

Het **EU-Internetforum**[68], waarbinnen al wordt samengewerkt door de lidstaten, de internetsector en andere partners, kan dienen als een ruimte waar op EU-niveau directe contacten en vertrouwen tussen betrokken actoren tot stand kunnen worden gebracht met betrekking tot activiteiten op het gebied van de toegang tot digitale gegevens. Het zou kunnen bijdragen tot het opzetten en actueel houden van een **open catalogus** van de soorten gegevens die aanbieders en gegevensverwerkers verzamelen en verwerken, eventueel met centraal beheer door Sirius. Een dergelijke catalogus zou het huidige gebrek aan transparantie verhelpen en de rechtshandhavings- en rechterlijke instanties meer duidelijkheid verschaffen over welke gegevens zij kunnen opvragen. Hij zou ook kunnen fungeren als coördinatiecentrum om te bepalen aan wie een verzoek moet worden gericht. In gevallen waarin er wettelijke verplichtingen worden opgelegd aan aanbieders, zou de catalogus daarnaast een meerwaarde bieden in termen van het monitoren en beoordelen van de uitvoering van transparantieverplichtingen met betrekking tot de soorten gegevens die aanbieders opslaan of anderszins verwerken.

---

65 Het Sirius-netwerk van centrale contactpunten, dat deskundigen op het gebied van rechtmatige verzoeken om gegevens groepeert, bevordert beste praktijken en moedigt landen aan hun eigen centrale contactpunt op te zetten. Centrale contactpunten zijn aangewezen personen, eenheden of instellingen die verzoeken van overheidsinstanties centraliseren, beoordelen, en indienen bij dienstverleners. Momenteel maken 36 rechtshandhavingsinstanties uit 25 landen deel uit van dit netwerk.

66 Het Sirius-project dient als aanspreekpunt voor het verkrijgen van elektronische gegevens van dienstverleners in andere rechtsgebieden. Sirius biedt een beperkt platform voor het delen van kennis en beste praktijken voor rechtshandhavingsinstanties en justitiële actoren. Het Sirius-project houdt een actueel register bij van contactgegevens van meer dan duizend ondernemingen, waarbij de focus ligt op kleinere, moeilijk te vinden of soms ontoegankelijke dienstverleners. Daardoor kunnen de bevoegde autoriteiten meerdere adressen opvragen in één handeling en kunnen zij op efficiëntere wijze omgaan met grote hoeveelheden complexe informatie. Sirius-project | Europol (europa.eu).

67 Sirius is een door de EU gefinancierd project dat rechtshandhavings- en rechterlijke instanties helpt toegang te krijgen tot grensoverschrijdend elektronisch bewijsmateriaal in het kader van strafrechtelijke onderzoeken en procedures. Het Sirius-project, dat gezamenlijk wordt uitgevoerd door Europol en Eurojust, in nauwe samenwerking met het EJN, is een centraal referentiepunt in de EU voor het delen van kennis over grensoverschrijdende toegang tot elektronisch bewijsmateriaal. Sirius-project | Europol (europa.eu).

68 EU-Internetforum (EUIF) – Europese Commissie (europa.eu).

Synergieën met het pakket elektronisch bewijsmateriaal kunnen kosten en middelen besparen en bijdragen tot de volledige uitvoering van de wetgeving inzake elektronisch bewijsmateriaal.
Zo zouden rechtshandhavingsinstanties ook voor verzoeken op nationaal niveau kunnen worden aangemoedigd om (extra) capaciteit te creëren voor eenheden die als centraal contactpunt optreden voor (grensoverschrijdende) verzoeken om openbaarmaking van gegevens, of zouden zij kunnen worden verplicht opleidingsprogramma's voor onderzoekers en eerstelijnsfunctionarissen aan te bieden. Evenzo zouden de inspanningen die momenteel in het kader van de uitvoering van het pakket elektronisch bewijsmateriaal worden geleverd om een **digitaal platform** op te zetten dat rechtstreekse uitwisselingen tussen bevoegde autoriteiten en aanbieders mogelijk maakt, kunnen worden uitgebreid tot communicatiemetagegevens die worden bewaard op grond van nationale wetgeving.

De lidstaten zouden **memoranda van overeenstemming** kunnen overwegen als instrument om de samenwerking te bevorderen en tot een gemeenschappelijke visie tussen dienstverleners, overheidsdiensten en rechtshandhavingsinstanties te komen ter ondersteuning van de uitvoering van nationale wetgeving. De positieve voorbeelden in sommige lidstaten kunnen inspiratie bieden voor de structuur van die memoranda, zodat alle relevante actoren (ondernemingen, agentschappen enz.) erbij worden betrokken en alle relevante aspecten van de samenwerking aan bod komen (aanwijzing van centrale contactpunten voor dienstverleners en rechtshandhavingsinstanties, technische behoeften, gemeenschappelijke definitie van de categorieën van te verstrekken gegevens, gezamenlijke procedures, opstellen van gestandaardiseerde modellen voor verzoeken, maatregelen voor gegevensbeveiliging en gegevensminimalisatie enz.)[69]. Zoals reeds opgemerkt, zouden **gestandaardiseerde protocollen** voor het verzamelen van gegevens bij aanbieders (met inbegrip van OTT-dienstverleners) en voor het opvragen van gegevens door bevoegde autoriteiten voordelen bieden voor zowel rechtshandhavingsinstanties als dienstverleners, die het verstrekken van antwoorden zouden kunnen automatiseren en zo kosten en tijd kunnen besparen. Hoewel de vereisten voor **nationale** en **grensoverschrijdende verzoeken** (binnen het kader voor elektronisch bewijsmateriaal) verschillen, is het mogelijk om workflows en kanalen voor het opvragen van gegevens te ontwikkelen, aangezien de normalisatie betrekking heeft op het formaat van de gevraagde/ontvangen gegevens. Normalisatie-instellingen zoals het ETSI verkeren in de beste positie om zo'n gestandaardiseerde formaten te ontwikkelen. Tot dusver zijn echter nog maar weinig rechtshandhavingsdeskundigen van de lidstaten bij deze processen betrokken. Daarom zou de bestaande **Europese werkgroep voor normalisatie inzake interne veiligheid**, die onder leiding staat van Europol en de Commissie, de deelname van de lidstaten aan dergelijke fora kunnen coördineren en aanmoedigen. De werkzaamheden zouden kunnen voortbouwen op bestaande door het ETSI ontwikkelde normen, die kunnen worden uitgebreid tot andere gegevenscategorieën[70].

---

[69] Het Ierse memorandum van overeenstemming van 6 april 2024 moet de uitvoering van de Communications (Retention of Data) Act 2011 (zoals gewijzigd) ondersteunen. Het Ministerie van Justitie heeft een onafhankelijke voorzitter benoemd, een mandaat vastgesteld en vertegenwoordigers van rechtshandhavingsinstanties en dienstverleners uitgenodigd.

[70] TS 102 657: verwerking van bewaarde gegevens; overdrachtsinterface voor het opvragen en verstrekken van bewaarde gegevens en categorieën bewaarde gegevens (gegevens over abonnees, gebruik, apparatuur, netwerkelementen en facturering); TS 103 120: interface voor informatie in het kader van een bevel (omschrijft een elektronische interface tussen twee systemen voor de beveiligde uitwisseling van informatie in verband met de vaststelling en het beheer van de nodige rechtmatige handelingen; gewoonlijk gebruikt voor legale intercepties, maar kan ook worden gebruikt voor bewaarde gegevens; gewoonlijk gebruikt tussen, aan de ene kant, een dienstverlener en, aan de andere kant, een overheidsdienst of rechtshandhavingsinstantie die gerechtigd is om een rechtmatige handeling aan te vragen); TS 103 705: gegevensstructuren voor rechtmatige openbaarmaking (in ontwikkeling; alleen gegevensstructuren, geen overdrachtsinterface, geen vooraf gedefinieerde boomstructuur, door de dienstverlener omschreven typen en informatie).

Kernactie: de GHN-deskundigen pleiten voor de bevordering van samenwerking en de ontwikkeling van een gemeenschappelijke visie tussen dienstverleners, overheidsdiensten en rechtshandhavingsinstanties

Actoren: Europese Commissie, lidstaten, Europol (Sirius), Eurojust, EU-Internetforum

Tijdschema: nog te bepalen

- De GHN-deskundigen verzoeken de **Europese Commissie, Europol** en de **lidstaten** na te gaan hoe de samenwerking tussen rechtshandhavingsinstanties en particuliere ondernemingen kan worden bevorderd en versterkt, waarbij een permanente dialoog en wederzijds begrip van operationele, technische en zakelijke behoeften worden gestimuleerd. De GHN-deskundigen verzoeken de Commissie ook in het kader van de in deel II vermelde effectbeoordeling na te denken over de ontwikkeling van specifieke verplichtingen inzake transparantie bij gegevensverzameling en permanente samenwerkingsstructuren.

- De GHN-deskundigen verzoeken de **Europese Commissie**, **Europol** en **Eurojust** om platforms op te zetten of bestaande platforms te bevorderen met het oog op uitwisselingen tussen rechtshandhavingsinstanties en justitie, enerzijds, en aanbieders van communicatiediensten, anderzijds, teneinde een door Sirius te beheren catalogus op te stellen van de gegevens die door aanbieders van communicatiediensten en gegevensverwerkers worden gegenereerd en opgeslagen in het kader van hun bedrijfsactiviteiten.

- De GHN-deskundigen verzoeken de **lidstaten** na te gaan of samenwerkingsovereenkomsten en/of memoranda van overeenstemming kunnen worden opgezet om dienstverleners, overheidsdiensten en rechtshandhavingsinstanties samen te brengen ter ondersteuning van de uitvoering van nationale wetgeving door het vaststellen van gemeenschappelijke beginselen en standaardpraktijken.

- De GHN-deskundigen verzoeken **Europol** en de **Europese Commissie** een beroep te doen op de bestaande werkgroep voor normalisatie inzake interne veiligheid om de deelname van de lidstaten aan normalisatiefora aan te moedigen zodat zij mee desbetreffende normen vaststellen en samen protocollen ontwerpen waarin de procedures voor samenwerking met dienstverleners nader worden beschreven.

- De GHN-deskundigen verzoeken de **Europese Commissie**, **Europol**, **Eurojust/het EJN** en de **lidstaten** gebruik te maken van synergieën met instrumenten zoals het pakket elektronisch bewijsmateriaal om relevante instrumenten te ontwikkelen of aan te schaffen, bijvoorbeeld door digitale platforms in ontwikkeling ook te gebruiken als portaal voor het indienen van verzoeken.

II. Geharmoniseerde minimumvoorschriften voor de bewaring van metagegevens door aanbieders van communicatiediensten en de toegang door bevoegde autoriteiten

De deskundigen zijn het er grotendeels over eens dat er behoefte is aan een geharmoniseerd EU-kader met regels inzake de bewaring van metagegevens voor rechtshandhavingsdoeleinden. Een dergelijk kader zou voorzien in gestandaardiseerde oplossingen en in duidelijke en afdwingbare verplichtingen voor aanbieders van communicatiediensten en gegevensverwerkers over wanneer en hoe zij gegevens moeten bewaren en onder welke omstandigheden zij toegang tot die gegevens moeten verlenen.
Dit kader zou, aan de hand van duidelijke regels inzake bewaring en toegang, duidelijke waarborgen bieden voor de grondrechten en voor wezenlijke belangen, rekening houdend met de toepasselijke jurisprudentie. Het zou ook duidelijkheid verschaffen over de regels die van toepassing zijn op aanbieders van communicatiediensten voor het bewaren en delen van gegevens voor rechtshandhavingsdoeleinden. Bovendien zou een dergelijk kader, door ervoor te zorgen dat gegevens worden bewaard, de volledige uitvoering van het pakket elektronisch bewijsmateriaal ondersteunen.

Aanbevelingscluster 6

Om de beschikbaarheid te waarborgen van het nodige digitale bewijsmateriaal voor het onderzoeken en vervolgen van strafbare feiten, om versnippering tussen de lidstaten te vermijden wat betreft de regels voor bewaring en de waarborgen met betrekking tot de grondrechten, met name privacy en de bescherming van persoonsgegevens, de vrijheid van meningsuiting en de rechten van de verdachte, met inbegrip van het recht op een eerlijk proces, en om rechtszekerheid te waarborgen voor zowel de bevoegde autoriteiten als de aanbieders van elektronische- en andere communicatiediensten, bevelen de deskundigen het volgende aan:

1. *categorieën metagegevens definiëren op basis van het doel van het gebruik ervan (in kaart brengen, lokaliseren, vaststellen of beoordelen van de onlineactiviteit van een persoon van belang) [aanbeveling 28], om ervoor te zorgen dat aanbieders van elektronische- en andere communicatiediensten op zijn minst voldoende gegevens bewaren om een persoon van belang te kunnen identificeren [aanbeveling 27, punt v)];*
2. *minimumtermijnen voor de bewaring van dergelijke gegevens vaststellen;*
3. *voorwaarden uitwerken voor de toegang tot bewaarde gegevens [aanbeveling 27, punt iv)] die verschillen naargelang de gegevenscategorie, de categorie strafbare feiten (bv. strafbare feiten die alleen op internet plaatsvinden) of de dreiging voor slachtoffers [aanbeveling 29];*
4. *wettelijke, regelgevende en technische bepalingen op zodanige wijze uitwerken dat deze de volledige eerbiediging van de fundamentele rechten en vrijheden van de betrokkenen volledig waarborgen en dat elke beperking van die rechten noodzakelijk en evenredig is [aanbeveling 27, punt vi)];*
5. *ervoor zorgen dat dezelfde regels, verplichtingen en waarborgen gelden voor traditionele aanbieders van communicatiediensten, aanbieders van OTT-diensten en alle andere bestaande of toekomstige aanbieders die gegevens genereren en verwerken [aanbeveling 27, punten i) en ii)];*
6. *ervoor zorgen dat gebruikersgegevens die voor commerciële en zakelijke doeleinden worden bewaard, goed toegankelijk zijn voor rechtshandhavingsinstanties, met inachtneming van de desbetreffende waarborgen (aanbeveling 31), en dat gegevens die rechtmatig van aanbieders zijn ontvangen, leesbaar zijn voor de bevoegde autoriteiten [aanbeveling 27, punt iii)];*
7. *ervoor zorgen dat de lidstaten sancties kunnen opleggen als aanbieders van elektronische- en andere communicatiediensten weigeren om gegevens te bewaren en te verstrekken, bijvoorbeeld door de invoering van administratieve sancties of beperkingen om op de EU-markt actief te zijn [aanbeveling 30].*

Als het gaat om de **bewaring van metagegevens**, moet een onderscheid worden gemaakt tussen verschillende categorieën gegevens. Gegevens die nodig zijn om een persoon van belang te identificeren (abonneegegevens[71] en IP-adressen van de bron van de communicatie[72]), moeten worden onderscheiden van verkeers-[73] en locatiegegevens[74], en per categorie moeten verschillende bewaartermijnen en waarborgen gelden. Ook met betrekking tot de toegang tot gegevens moet een evenwicht worden gevonden tussen de ernst van het te onderzoeken strafbare feit en de mate waarin de te nemen maatregelen inbreuk maken op de privacy. In lijn met recente jurisprudentie[75] zouden minimumvereisten kunnen worden onderzocht voor een generieke gegevensbewaring die volstaat om elke gebruiker duidelijk te identificeren. Voor verkeers- en locatiegegevens moeten aanvullende en strengere criteria worden onderzocht.

Om een dergelijk kader zo toekomstbestendig en **technologieneutraal** mogelijk te maken, moet bij de categorisering van de te bewaren gegevens een toekomstgerichte benadering worden gevolgd, met onder meer generieke datasets die bijvoorbeeld gebaseerd zijn op de functies van de gegevens (gegevens aan de hand waarvan een communicatiebron of -bestemming op unieke wijze kan worden geïdentificeerd, gegevens aan de hand waarvan de locatie van een communicatiebron kan worden nagegaan enz.), in combinatie met een lijst van bestaande gegevenstypen (IP-adres, IMEI enz.). Met een dergelijk kader zou de indringendheid van elke gegevenscategorie – en dus de vereiste waarborgen – goed kunnen worden beoordeeld.

---

71 Op enkele uitzonderingen voor kleine aanbieders na worden gebruikersgegevens over het algemeen al bewaard voor zakelijke doeleinden. Wanneer dit het geval is, moeten die gegevens, zonder afbreuk te doen aan evenredige waarborgen, ter beschikking worden gesteld van rechtshandhavingsinstanties.

72 De rechtspraak staat de algemene en ongedifferentieerde bewaring toe van gegevens inzake de burgerlijke identiteit van gebruikers van elektronische communicatiediensten met het oog op de bescherming van het algemeen belang, alsook de algemene en ongedifferentieerde bewaring van IP-adressen met het oog op de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid (arrest van 6 oktober 2020, La Quadrature du Net e.a., gevoegde zaken C-511/18, C-512/18 en C-520/18, en arrest van 30 april 2024, La Quadrature du Net e.a., zaak C-470/21 (“zaak Hadopi”), ECLI:EU:C:2024:370).

73 Onder “verkeersgegevens” wordt verstaan: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronischecommunicatienetwerk of voor de facturering ervan (artikel 2 van Richtlijn 2002/58/EG).

74 Onder “locatiegegevens” wordt verstaan: gegevens die in een elektronischecommunicatienetwerk worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronischecommunicatiedienst wordt aangegeven (artikel 2 van Richtlijn 2002/58/EG); locatiegegevens van de apparatuur van de gebruiker moeten worden beschouwd als de in artikel 9 van Richtlijn 2002/58/EG bedoelde andere locatiegegevens dan verkeersgegevens.

75 Arrest Hadopi.

Volgens de deskundigen en de recente rechtspraak[76] zou het combineren van bewaarverplichtingen met strenge **eisen inzake toegang tot gegevens** extra waarborgen bieden voor de grondrechten, met name privacy en de bescherming van persoonsgegevens. De GHN-deskundigen hebben dan ook onderzocht of toegangsregels moeten worden opgesteld die bijvoorbeeld verschillen naargelang het soort en de ernst van het strafbare feit, het niveau van de dreiging die het strafbare feit inhoudt voor de slachtoffers, het doel van de toegang, en de autoriteiten die gerechtigd zijn om toegang tot de gegevens te krijgen. Een dergelijke benadering werd ook beschouwd als een nuttige manier om specifieke regels vast te stellen voor het onderzoeken en vervolgen van misdrijven die bijzonder moeilijk te onderzoeken zijn, zoals strafbare feiten die uitsluitend op het internet worden gepleegd en waarbij alleen digitaal bewijsmateriaal beschikbaar is.

Zodra rechtmatige toegang tot gegevens is verkregen, moeten de gegevens leesbaar zijn voor de verzoekende autoriteiten. Daarom moeten de aanbieders de gegevens in een **begrijpelijk formaat** verstrekken. Vaak bieden aanbieders diensten met eind-tot-eindencryptie[77] voor verkeers- en abonneegegevens aan, en delen zij die gegevens met de bevoegde autoriteiten zonder ze eerst te decrypteren. De GHN-deskundigen waren van mening dat een regeling voor gegevensbewaring de dienstverleners ertoe moet verplichten gegevens ongecodeerd te verstrekken en tegelijkertijd borg moet staan voor een sterke cyberbeveiliging en een volledige naleving van de wetgeving inzake privacy en gegevensbescherming, zonder encryptie te ondermijnen.

Voor een doeltreffend kader voor gegevensbewaring, zowel nu als in de toekomst, zouden minimumeisen voor de bewaring van specifieke categorieën gegevens moeten gelden (en afdwingbaar moeten zijn) voor elke (huidige of toekomstige) marktdeelnemer die elektronischecommunicatiediensten verstrekt. Om rekening te houden met toekomstige technologische ontwikkelingen moeten de verplichtingen inzake gegevensbewaring ook van toepassing zijn op telecommunicatieaanbieders, OTT-aanbieders en andere exploitanten – zoals autofabrikanten of AI-systemen op basis van een LLM – die gegevens verzamelen over een specifieke natuurlijke persoon of rechtspersoon die gebruik maakt van hun dienst. Deze verplichtingen moeten afdwingbaar zijn en aanbieders moeten ter verantwoording kunnen worden geroepen. Dit kan op verschillende manieren worden bereikt, bijvoorbeeld aan de hand van marktbelemmeringen (exploitatievergunningen) of administratieve sancties.

---

[76] In de recente zaak Hadopi heeft het Hof geconcludeerd dat de privacy kan worden gewaarborgd door een combinatie van bewaring en toegang.

[77] Zie deel I.

Een systeem van afdwingbare sancties voor niet-meewerkende aanbieders en aanbieders die illegale diensten hosten, is een essentieel aspect van elk toekomstig EU-kader. Gezien de wisselwerking tussen dit specifieke aspect en de mogelijke oplossingen die in het kader van legale interceptie zijn besproken, moeten sancties aan bod komen tijdens de volgende vergadering over legale interceptie.

Hoewel voor de meeste aanbieders de verplichting om gegevens te bewaren en te verstrekken voornamelijk technische uitvoering zou behelzen (d.w.z. het ter beschikking stellen van voor zakelijke doeleinden verzamelde of verwerkte gegevens aan de bevoegde autoriteiten), zou dit betekenen dat standaardprocedures voor de registratie van gebruikers worden opgelegd aan aanbieders die hun gebruikers momenteel niet registreren omdat zij daar geen zakelijke belangen bij hebben (zoals OTT-aanbieders). Dit soort verplichtingen werd door de GHN-deskundigen als positief beschouwd tijdens de besprekingen over de noodzaak om de **transparantie en de verantwoordingsplicht** van aanbieders te vergroten met betrekking tot de door hen verzamelde en opgeslagen gegevens en de opslagduur. Bestaande verplichtingen voor categorisatie in het kader van andere instrumenten (AVG) kunnen inzicht verschaffen in de door deze aanbieders verwerkte gegevens.

Kernactie: de GHN-deskundigen pleiten voor een nieuw EU-kader voor gegevensbewaring en -toegang

Actoren: Europese Commissie, Raad, Europees Parlement

Tijdschema: 2025-2026

- De GHN-deskundigen dringen er bij de **Europese Commissie** op aan dat zij van start gaat met een effectbeoordeling met het oog op de evaluatie van verschillende opties die de bevoegde autoriteiten beter in staat kunnen stellen om strafbare feiten doeltreffend te onderzoeken en te vervolgen aan de hand van toegang tot historische metagegevens die door aanbieders van communicatiediensten zijn gegenereerd en opgeslagen. De effectbeoordeling moet ook betrekking hebben op de subsidiariteitsvereisten, de gevolgen voor de grondrechten en de interne markt, en het verband met andere bestaande rechtsinstrumenten. Zij moet als basis dienen voor een wetgevingsvoorstel, dat volgens de gewone wetgevingsprocedure moet worden aangenomen.

Hoofdstuk III: legale interceptie

WAAR GAAT HET OM?

"Legale interceptie van communicatie" doet zich voor wanneer een derde – een autoriteit of een andere entiteit die daartoe door of op basis van een wet is gemachtigd – heimelijk toegang krijgt tot gegevens uit een verdachte communicatie. Terwijl legale interceptie in het verleden vooral relevant was voor telefoongesprekken, heeft de toenemende verschuiving van traditionele telefoongesprekken naar berichtendiensten en andere vormen van elektronische communicatie tot nieuwe uitdagingen geleid.

Deze verschuiving is tot uiting gebracht in het EECC door een deel van het rechtskader voor traditionele telecommunicatie uit te breiden tot bedrijven die internetdiensten aanbieden via een telecommunicatie-infrastructuur die zij niet in eigendom of beheer hebben, waaronder nummeronafhankelijke interpersoonlijke communicatiediensten (*number-independent interpersonal communications services* of NI-ICS). In de praktijk betekent dit dat NI-ICS-aanbieders onderworpen kunnen worpen aan het rechtskader dat al van toepassing was op traditionele telecommunicatiebedrijven, ook wat betreft legale interceptie. De lidstaten kunnen eisen dat exploitanten legale interceptie van elektronische communicatie door nationale bevoegde autoriteiten toestaan uit hoofde van Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, die bepalingen inzake vertrouwelijkheid van communicatie en de uitzonderingen daarop bevatten. De lidstaten kunnen die eis ook stellen in het kader van de algemenemachtigingsregeling van het EECC.

Rechtmatige toegang hoeft niet plaats te vinden op netwerkniveau – zoals het geval was voor traditionele telefoongesprekken en tekstberichten (sms) – maar kan ook gebeuren op het apparaat van de gebruiker (voordat de informatie wordt verzonden) of op de bestemming (bv. wanneer berichten in de cloud worden opgeslagen). In de context van dit verslag heeft legale interceptie betrekking op deze drie gebruiksgevallen en op gegevens waartoe in real time of met weinig vertraging toegang wordt verkregen.

Er moet een onderscheid worden gemaakt tussen interceptietechnologieën die worden **toegepast door een communicatie-exploitant** en technologieën die autonoom door rechtshandhavingsinstanties kunnen worden ingezet. Alleen de eerstgenoemde vorm van interceptie [in dit verslag "**interceptie via de exploitanten**" genoemd], waarbij de communicatie-exploitant technische systemen moet installeren om de onderschepte gegevens te verzamelen en aan de verzoekende autoriteiten te verstrekken, is opgenomen in de definitie van "legale interceptie" in de ETSI-normen. De laatstgenoemde vorm [in dit verslag "**tactische interceptie**" genoemd] heeft betrekking op instrumenten die geen permanente fysieke installatie op een netwerk vereisen, zoals IMSI-catchers[78] of software voor het onderscheppen van gegevens op smartphones. Met deze gebruikssituaties zijn verschillende niveaus van indringendheid en uitdagingen van verschillende aard gemoeid, en zij vallen niet onder dezelfde wettelijke regeling.

Hoewel legale interceptie van traditionele telecommunicatie nog steeds een essentieel instrument is in veel onderzoeken[79], is de doeltreffendheid van deze maatregel drastisch afgenomen omdat telecommunicatiediensten nu meestal worden geleverd door andere actoren. Volgens verschillende bronnen wordt ongeveer 97 % van alle mobiele berichten nu verzonden via berichtenapps zoals WhatsApp, Facebook Messenger en WeChat, terwijl traditionele sms- en mms-berichten slechts goed zijn voor ongeveer 3 % van de berichten. Bovendien verliep in 2023 meer dan 90 % van de OTT-communicatie via diensten met eind-tot-eindencryptie[80].

Volgens de deskundigen heeft zich een trend voorgedaan waarbij criminelen eerst begonnen over te stappen van traditionele communicatie-exploitanten op reguliere OTT's. Vervolgens begonnen belangrijke criminele actoren geleidelijk gebruik te maken van specifieke criminele netwerken (zoals Encrochat en Sky ECC). Sinds 2020, toen grote criminele communicatienetwerken die beschermd waren met encryptie, werden verstoord, zijn velen van hen weer overgestapt op reguliere OTT's met eind-tot-eindencryptie.

---

78 IMSI-catchers zijn surveillanceapparaten die zendmasten voor mobiele telefonie nabootsen om mobiele telefoonsignalen op te pikken, waarbij IMSI-nummers (IMSI = *international mobile subscriber identity* – internationale identiteit mobiele abonnee) en communicatiegegevens worden onderschept.

79 De afgelopen jaren is het aantal verzoeken om legale interceptie in Europa aanzienlijk en gestaag toegenomen. In landen als Duitsland, Frankrijk en het Verenigd Koninkrijk lag het aantal dergelijke verzoeken bijzonder hoog, met alleen in Duitsland een opmerkelijke stijging. Zo meldde Deutsche Telekom in 2023 meer dan 31 000 interceptieverzoeken, tegenover ongeveer 26 000 in 2022 (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Bronnen: Comparitech en Statista.

In de geschetste context staan aanbieders van communicatiediensten voor zulke grote uitdagingen dat zij bij het beantwoorden van verzoeken om legale interceptie nauwelijks kunnen voldoen aan de essentiële eisen van legale interceptie zoals gedefinieerd in het Verdrag van Boedapest inzake cybercriminaliteit[81]. Daardoor is de operationele waarde van traditionele legale interceptie vaak beperkt tot tactische inzichten in de vraag of een apparaat aan of uit staat, waar de netwerkantenne zich bevindt, wie met wie in contact staat enz. Legale interceptie van inhoudelijke gegevens die via OTT-diensten worden verzonden, is echter meestal niet mogelijk.

Een en ander betekent dat rechtshandhavingsinstanties vaak geen toegang kunnen krijgen tot de inhoud van gerichte communicatie[82] en deze niet kunnen lezen, of zelfs niet kunnen weten wie een bepaalde internetdienst in real time aan het gebruiken is, noch relevante informatie kunnen filteren. Dit aanzienlijke verlies van toegang tot gegevens in doorvoer heeft verschillende gevolgen voor onderzoeken:

- grote moeilijkheden om strafbare feiten te voorkomen, criminele organisaties in kaart te brengen en na te gaan wie de dader is van online of offline gepleegde criminele activiteiten;

- toegenomen gebruik door rechtshandhavingsinstanties van zogenaamde speciale technieken[83], die vaak indringender zijn en veel gevaarlijker zijn voor politiefunctionarissen, bijvoorbeeld wanneer de gerechtelijke autoriteit de installatie van camera's of microfoons in de buurt van het doelwit beveelt;

- toegenomen gebruik door rechtshandhavingsinstanties van minder gerichte onderzoekstechnieken: zonder toegang tot communicatie-inhoud of precieze geolocatiegegevens moeten onderzoekers vaak **alle** personen onderzoeken die banden hebben met een persoon die van criminele activiteiten wordt verdacht.

Tegen die achtergrond hebben de GHN-deskundigen vier belangrijke categorieën van uitdagingen aangewezen.

---

81 https://rm.coe.int/1680081561 [art. 20 en 21].

82 Eén deskundige gaf aan dat inhoudelijke gegevens in 99 % van de gevallen niet beschikbaar zijn via traditionele legale interceptie.

83 De zogenaamde speciale technieken omvatten een reeks tactische middelen om informatie te verkrijgen over de beoogde persoon van belang door middel van camera's, microfoons, toegang op afstand tot apparaten, gps-trackers enz.

I. Legale interceptie van communicatie via niet-traditionele aanbieders van communicatiediensten

De meeste lidstaten hebben een of andere vorm van regelgeving ingevoerd voor legale interceptie, waarbij aanbieders van communicatiediensten worden verplicht te voorzien in interceptiecapaciteit[84]. Hoewel de voorwaarden voor het uitvaardigen van bevelen tot legale interceptie sterk verschillen van land tot land, zijn de verplichtingen voor exploitanten vaak vergelijkbaar[85]: zij moeten in staat zijn om alle relevante communicatie van een bepaald doelwit op het nationale grondgebied zonder onderbreking te onderscheppen en zij moeten over de nodige infrastructuur beschikken om de onderschepte gegevens te verzamelen en door te sturen naar de rechtshandhavingsinstanties.

Exploitanten van telecommunicatienetwerken (aanbieders van communicatiediensten die eigenaar zijn van het netwerk en toegang hebben tot de infrastructuur ervan) die ook communicatiediensten (telefoongesprekken, sms enz.) aanbieden, zijn meestal in staat om aan de verplichtingen inzake wettelijke interceptie te voldoen[86]. In de meeste gevallen baseren zij zich op ETSI-normen en doen zij een beroep op gespecialiseerde technologieleveranciers om hun verplichtingen te beheren, onder meer ten aanzien van kosteneffectiviteit, een minimale impact op de netwerkinfrastructuur, interoperabiliteit, betrouwbaarheid en beveiliging.

Voor OTT-diensten is de situatie complexer: legale interceptie kan worden uitgevoerd door de exploitant van een telecommunicatienetwerk of door de OTT-aanbieder die de dienst levert.

Interceptie van communicatie via OTT-diensten op het niveau van het telecommunicatienetwerk is vaak niet zo doeltreffend. Om te beginnen kan de exploitant van het telecommunicatienetwerk misschien niet nagaan welke communicatie afkomstig is van het doelwit (bv. wanneer verbinding wordt gemaakt via openbare wifi). Daarnaast maken OTT-diensten vaak gebruik van eigen protocollen, die door legale-interceptiesystemen moeten worden gedecodeerd, wat extra kosten, tijd en complexiteit meebrengt. Tot slot maakt het gebruik van eind-tot-eindencryptie door OTT-aanbieders het bijzonder lastig om toegang tot inhoudelijke gegevens te verkrijgen en verhindert het in toenemende mate de toegang tot metagegevens. In lijn met het Verdrag van Boedapest is een grote meerderheid van de landen immers van mening dat exploitanten van telecommunicatienetwerken niet kunnen worden verplicht om informatie ongecodeerd te verstrekken indien de gegevens zijn geëncrypteerd door een derde.

---

84 Zie "Lawful interception – A market access barrier in the European Union", Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

85 Er zijn wel verschillende verplichtingen naargelang het gaat om inhoudelijke of niet-inhoudelijke gegevens.

86 Hoewel functies zoals homerouting, slicing of Rich Communication Services het moeilijker kunnen maken voor exploitanten van telecommunicatienetwerken om hun verplichtingen na te komen (zie het deel over technologische uitdagingen).

In artikel 5, lid 1, van de e-privacyrichtlijn wordt verwezen naar de definitie van "elektronischecommunicatiediensten" in het EECC, die sinds 2018 ook NI-ICS omvat. Dankzij de verruiming van de definitie van elektronischecommunicatiediensten (ten opzichte van het moment waarop de e-privacyrichtlijn werd vastgesteld) kunnen de lidstaten zich nu rechtstreeks tot OTT-aanbieders richten voor legale interceptie[87]. Tot op heden hebben de lidstaten niet in dezelfde mate gebruik gemaakt van deze mogelijkheid. Sommige lidstaten hebben soortgelijke verplichtingen vastgesteld voor alle soorten aanbieders van elektronischecommunicatiediensten, inclusief OTT-aanbieders, terwijl andere lidstaten OTT-aanbieders uitsluiten[88]. **In de praktijk hebben reguliere OTT-diensten, ondanks de bestaande verplichtingen, geen technische mechanismen ontwikkeld om te reageren op verzoeken om legale interceptie vanwege de autoriteiten van EU-lidstaten**, voornamelijk om juridische redenen[89].

Daarentegen heeft het VK met de Investigatory Powers Act een kader voor legale interceptie van OTT-communicatie opgetuigd, dat dankzij de overeenkomst inzake gegevenstoegang tussen het VK en de VS ook van toepassing is op in de VS gevestigde aanbieders van OTT-diensten. Volgens de bevoegde Britse autoriteiten maakt dit een aanzienlijk verschil voor criminaliteitspreventie en strafrechtelijke onderzoeken.

Tot slot hebben deskundigen van nationale autoriteiten duidelijk gemaakt dat tactische interceptie, gebaseerd op het benutten van kwetsbaarheden, geen doeltreffend of wenselijk alternatief is voor afdwingbare regels voor legale interceptie die van toepassing zijn op OTT-aanbieders, en beperkt moet blijven tot specifieke gevallen, met sterke garanties in de nationale wetgeving om evenredigheid te waarborgen.

---

87 Hoewel er nog besprekingen gaande zijn over de precieze reikwijdte van de toepasbaarheid, en de interpretaties van lidstaat tot lidstaat verschillen.

88 Zie "Lawful interception – A market access barrier in the European Union", Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

89 Dit wordt niet gestaafd door statistieken aangezien de nationale autoriteiten zeer zelden verzoeken om legale interceptie naar OTT-aanbieders sturen, omdat zij zich er terdege van bewust zijn dat dit waarschijnlijk geen resultaten zal opleveren.

II. Grensoverschrijdende verzoeken

Grensoverschrijdende verzoeken om legale interceptie gericht aan aanbieders van OTT-diensten en – in mindere mate – aan traditionele aanbieders van communicatiediensten brengen verschillende uitdagingen met zich mee voor rechtshandhavingsinstanties.

Wat traditionele aanbieders van communicatiediensten betreft, worden de instanties in de eerste plaats geconfronteerd met organisatorische uitdagingen. Ten eerste kunnen internationale samenwerkingsinstrumenten – met name mechanismen voor wederzijdse rechtshulp – onpraktisch zijn voor dringende intercepties die binnen enkele uren, en dus niet enkele dagen of weken[90], toestemming en uitvoering vereisen. Dit is te wijten aan het aantal stappen dat moet worden ondernomen om de naleving van de wetgeving in zowel de verzoekende als de ontvangende lidstaat te waarborgen. De algemene perceptie is dat het proces van wederzijdse rechtshulp inefficiënt en belastend is wanneer het wordt toegepast op legale interceptie. Het Europees onderzoeksbevel (EOB), dat in 2017 van toepassing is geworden, verving de traditionele procedures voor wederzijdse rechtshulp in de EU[91] door strikte termijnen[92] vast te stellen voor het verzamelen van het gevraagde bewijsmateriaal, de gronden voor het weigeren van dergelijke verzoeken te beperken en één standaardformulier in te voeren waarmee autoriteiten kunnen verzoeken om hulp bij het verkrijgen van bewijsmateriaal. Wanneer bij de uitvoering van de interceptie geen technische bijstand nodig is van de lidstaat waar de persoon op wie de interceptie betrekking heeft zich bevindt, wordt die lidstaat bovendien in kennis gesteld van de interceptie door middel van een standaardformulier en krijgt die lidstaat de kans om er binnen 96 uur bezwaar tegen te maken. In baanbrekende zaak C-670/22 heeft het HvJ-EU een ruime interpretatie van "interceptie van telecommunicatie" gehanteerd en geoordeeld dat de infiltratie van eindapparatuur voor het verzamelen van verkeers-, locatie- en communicatiegegevens van een onlinecommunicatiedienst geldt als een "interceptie van telecommunicatie". De deskundigen zijn echter van mening dat de aanzienlijke verbeteringen die het EOB heeft teweeggebracht ontoereikend zijn om tegemoet te komen aan de behoefte aan snelle en geharmoniseerde grensoverschrijdende toegang tot gegevens in beweging.

Bovendien meldden de autoriteiten van de lidstaten dat de bestaande technische architectuur vaak niet geschikt is om legale interceptie in een lidstaat uit te voeren en de gegevens in bijna realtime door te geven aan een andere lidstaat. In sommige gevallen, wanneer er relevante organisatorische protocollen bestaan, is de hoeveelheid over te dragen gegevens eenvoudigweg niet verenigbaar met de bandbreedte die beschikbaar is via beveiligde communicatiekanalen.

---

[90] Deskundigen noemden gevallen waarin de zaak voorbij was voordat de grensoverschrijdende legale interceptie daadwerkelijk werd uitgevoerd of gevallen waarin de achterstand op het vlak van wederzijdse rechtshulp meer dan 8 maanden bedroeg.

[91] Met uitzondering van DK en IE, waar het EOB niet van toepassing is.

[92] 30 dagen voor de erkenning van een EOB en 90 extra dagen voor de tenuitvoerlegging ervan.

Het onderscheppen van OTT-communicatie brengt complexe bevoegdheidskwesties met zich mee in vergelijking met de interceptie van telefoongesprekken, waarbij aanbieders hun diensten verlenen op een duidelijk afgebakend grondgebied. Traditionele telecommunicatiediensten zijn gekoppeld aan een specifieke fysieke netwerkinfrastructuur, waardoor de dienstverlener over faciliteiten en een legale aanwezigheid moet beschikken in het land waar de interceptie plaatsvindt. Deze plaatsgebonden opzet vermindert het risico op juridische conflicten binnen de EU en maakt naleving eenvoudiger.

In het geval van OTT-diensten daarentegen kunnen de verzoekende autoriteit, het doelwit van de interceptie, de materiële uitvoering en de plaats van vestiging van de onderneming zich in verschillende rechtsgebieden bevinden. De interactie tussen de rechtskaders in deze rechtsgebieden zou kunnen leiden tot wetsconflicten[93].

Bij deskundigen van politiële en justitiële autoriteiten bestaat er geen twijfel: het uitvoeren van verzoeken om legale interceptie via internationale instrumenten is geen haalbare oplossing. Als rechtshandhavingsinstanties de procedure voor wederzijdse rechtshulp omzeilen en in plaats daarvan rechtstreeks bevelen aan dienstverleners richten op grond van hun nationale wetgeving, kunnen OTT-aanbieders zoals Microsoft, Meta of Google te maken krijgen met tegenstrijdige wettelijke vereisten. Zo zouden in veel verzoekende lidstaten regels inzake rechtmatige toegang gelden die in strijd zijn met het Ierse recht[94], dat van toepassing is op verschillende in Ierland gevestigde grote OTT-aanbieders, die echter ook onder het nationale recht kunnen vallen van de lidstaten waar zij hun diensten aanbieden.

Deze uitdagingen kunnen doeltreffend worden aangepakt door middel van gezamenlijke maatregelen en een zekere mate van harmonisatie van de regels inzake legale interceptie op EU-niveau, teneinde grensoverschrijdende verzoeken om legale interceptie te vergemakkelijken en te versnellen. Dit is tevens een voorwaarde voor het aanpakken van andere uitdagingen van organisatorische en technische aard, waarvoor oplossingen kunnen worden gevonden wanneer duidelijke en werkbare regels zijn vastgesteld.

---

93 Zie "LE interception concerns under the EECC", Microsoft, januari 2020.

94 Het Ierse recht verbiedt live intercepties door OTT-aanbieders.

III. Technologie

Ongeacht juridische overwegingen hebben ontwikkelingen op het gebied van communicatietechnologieën een invloed op de technische capaciteit van rechtshandhavingsinstanties om communicatie te onderscheppen via diensten die rechtstreeks door aanbieders van communicatiediensten of aanbieders van OTT-diensten worden geleverd.

Voor traditionele aanbieders van communicatie worden capaciteiten op het gebied van legale interceptie gewoonlijk ontwikkeld door technologieaanbieders op basis van ETSI-normen en opgenomen in 3GPP[95]. Daardoor kunnen goed uitgeruste politiediensten de interceptie van traditionele communicatie – spraak- en sms-berichten – naar behoren afhandelen en kunnen zij mogelijk internetcommunicatie via door hun netwerken aangeboden diensten onderscheppen.

De toenemende complexiteit van communicatie-infrastructuur en -protocollen in het kader van 5G, zoals virtualisering, netwerkslicing, edgecomputing en privacybevorderende functies, brengt echter nieuwe technologische uitdagingen met zich mee voor traditionele exploitanten[96]. De GHN-deskundigen legden met name de nadruk op uitdagingen op het gebied van homerouting[97] en Rich Communication Services (RCS)[98].

Vanuit een toekomstgericht perspectief en op basis van de ervaring met 5G verwachten de GHN-deskundigen uitdagingen in verband met de toekomstige uitrol van 6G (gepland voor na 2030). 6G zal nog een stap verder gaan op het gebied van privacybevorderende functies[99], met mogelijk eind-tot-eindencryptie als norm, waardoor, alles bij elkaar genomen, interceptie moeilijk zou kunnen worden. Tegelijkertijd brengen nieuwe communicatietechnologieën zoals IoT, satellietcommunicatie en de ontwikkeling van kwantumcomputing[100] nog andere uitdagingen met zich mee, waarop moet worden geanticipeerd.

---

95 Third Generation Partnership Project; hier wordt de basis gelegd voor de ontwikkeling van communicatietechnologieën zoals 5G, IoT en mobiele breedband.

96 Zie "Law enforcement and judicial aspects related to 5G", EU-coördinator voor terrorismebestrijding, 2019. https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol - Position paper on Home routing.pdf (europa.eu).

98 Via het RCS-protocol kunnen groepchats, video's, audio's en afbeeldingen met een hoge resolutie worden uitgewisseld; vaak wordt dit gebruikt in plaats van sms. Afhankelijk van de implementatie ervan kan de legale interceptie van RCS-berichten onmogelijk zijn, wat aanzienlijke gevolgen heeft voor de rechtshandhaving (in 2023 waren er meer dan 1 miljard actieve gebruikers van RCS).

99 Zie 6G roadmap: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf.

100 The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol (europa.eu).

Tot slot benadrukten de GHN-deskundigen dat eind-tot-eindencryptie, met name voor OTT-communicatie, een van de belangrijkste technische uitdagingen voor rechtshandhavingsinstanties is, en dat meer dan 80 % van de communicatie via diensten met eind-tot-eindencryptie (live communicatie en backup-opslag) verloopt, waardoor onderzoekers geen toegang hebben tot communicatie-inhoud. Tegelijkertijd zijn de deskundigen het erover eens dat eind-tot-eindencryptie een robuuste veiligheidsmaatregel is die burgers op een doeltreffende manier beschermt tegen verschillende vormen van criminaliteit. Door ervoor te zorgen dat alleen de communicerende gebruikers toegang hebben tot de inhoud van hun berichten, zorgt eind-tot-eindencryptie voor doeltreffende bescherming tegen onrechtmatig afluisteren, gegevensdiefstal, door de staat gesteunde spionage en andere vormen van ongeoorloofde toegang door hackers, cybercriminelen of zelfs de dienstverleners zelf.

Het is moeilijk om de uitdagingen te kwantificeren waarmee rechtshandhavingsinstanties worden geconfronteerd bij het monitoren van de communicatie van criminelen en terroristen waarbij eind-tot-eindencryptie is gebruikt. De reden hiervoor is dat rechtshandhavingsinstanties er vaak voor opteren geen tijd en middelen te investeren in het verkrijgen van rechterlijke bevelen voor elektronisch toezicht op platforms waarvan bekend is dat zij standaard eind-tot-eindencryptie gebruiken[101]; daarom ligt het aantal daadwerkelijke verzoeken om legale interceptie van inhoudelijke gegevens dat niet kan worden uitgevoerd vanwege eind-tot-eindencryptie zeer laag en zijn deze cijfers niet betekenisvol. De rechtshandhavingsinstanties zien dit gebrek aan capaciteit om toezicht te houden als een aanzienlijke blinde vlek en kwetsbaarheid. Criminelen en terroristen zijn zich hier ten volle van bewust en buiten dit actief uit, zoals blijkt uit de zaken EncroChat[102] en Sky ECC, die hebben geleid tot duizenden arrestaties in heel Europa, onder meer van een groot aantal criminele zwaargewichten. Deze bezorgdheid is tevens aan bod gekomen in verschillende verklaringen, onder meer van de Europese hoofden van politie[103] en de G7[104]. Om de gevolgen van het verlies van toegang tot inhoudelijke gegevens te illustreren, verwezen de deskundigen naar verschillende gekende voorbeelden van onder meer terrorisme[105], drugshandel[106] en verkrachting[107], waarbij encryptie het vermogen van rechtshandhavingsinstanties om zware en georganiseerde criminaliteit te voorkomen en te bestrijden, aanzienlijk belemmerde.

Rechtshandhavingsvertegenwoordigers geven de voorkeur aan een aanpak die ondernemingen verplicht om rechtshandhavingsinstanties onder strikte voorwaarden toegang tot niet-gecodeerde gegevens te bieden. Hierbij moet evenwel worden opgemerkt dat deskundigen op het gebied van cyberbeveiliging hun bezorgdheid hebben geuit over het feit dat dergelijke oplossingen de cyberbeveiliging zouden ondermijnen. Sommige rechtshandhavingsdeskundigen gaven aan dat encryptie in bepaalde gevallen is toegepast op een manier die verenigbaar is met zowel cyberbeveiliging als de noodzaak om bepaalde diensten te behouden, zoals updates van besturingssystemen, het scannen van inhoud (bv. e-mails of websessies) voor cyberbeveiligingsdoeleinden, of belangrijke herstelfuncties wanneer de gebruiker voor deze optie kiest.

---

101 Manpearl, 2017.

102 Voor meer informatie over EncroChat en Sky ECC, zie het verslag van Europol en Eurojust met als titel “Third Report of the Observatory Function on Encryption”, juni 2021.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version.

105 In maart 2017 voerde Khalid Masood, een 52-jarige man, een islamistisch geïnspireerde terreuraanslag uit in het centrum van Londen, waarbij zes mensen om het leven kwamen en 29 anderen gewond raakten. Hoewel uit verlagen van het incident bleek dat Masood zich alleen had voorbereid en alleen handelde, bleek dat hij, enkele minuten voordat hij de aanslag uitvoerde, een pdf-document met als titel “Jihad” naar een groot aantal van zijn contacten op WhatsApp en iMessage had gestuurd, die allebei standaard eind-tot-eindencryptie gebruikten en nog steeds gebruiken. Bronnen: Max Hill, “The Westminster Bridge Terrorist Attack” (London: The Stationery Office, 2018); BBC News, “WhatsApp Must Not Be a ‘Place for Terrorists to Hide’”, 26 maart 2017.

106 De deskundigen verwezen naar grootschalige gevallen van drugshandel waarbij geen vooruitgang kon worden geboekt voordat toegang werd verkregen tot via Encrochat en Sky ECC geëncrypteerde communicatie.

107 In een prominente zaak in het VK werden politieonderzoeken in een verkrachtingszaak belemmerd omdat verdachten WhatsApp gebruikten om te communiceren, en de eind-tot-eindencryptie het moeilijk maakte om toegang te krijgen tot cruciaal bewijsmateriaal. Het onvermogen van rechtshandhavingsinstanties om WhatsApp-berichten zonder toestemming van de gebruiker te decrypteren, belemmerde het onderzoek.

Op basis daarvan waren de rechtshandhavingsdeskundigen het erover eens dat de uitdagingen als gevolg van encryptie een veelzijdige aanpak vereisen waarbij een evenwicht wordt gevonden tussen privacyrechten, veiligheid en de noodzaak voor rechtshandhavingsinstanties om toegang te krijgen tot gegevens om criminaliteit te bestrijden en het leven, de fysieke integriteit en de eigendommen van mensen te beschermen. Hoewel het onwaarschijnlijk is dat een enkele oplossing alle punten van zorg zal wegnemen, zou een combinatie van benaderingen het probleem kunnen helpen beperken.

IV. Aanbieders van communicatie van criminele aard

Criminelen maken gebruik van platforms met eind-tot-eindencryptie om hun communicatie verborgen te houden. Ze kunnen echter ook gebruikmaken van beveiligde communicatiekanalen die specifiek zijn ontworpen voor criminele activiteiten (hierna "criminele communicatiekanalen")[108]. EncroChat en Sky ECC zijn beide bekende criminele communicatiekanalen die telefoons hebben verkocht met een geïntegreerde berichtendienst met eind-tot-eindencryptie die is ontworpen om criminele activiteiten te verhullen en die op het darkweb wordt gepromoot. Deze platforms werden in 2020 en 2021 ontmanteld dankzij gezamenlijke internationale rechtshandhavingsoperaties waaruit bleek dat zij op grote schaal gebruikt werden in het kader van georganiseerde criminaliteit. Verschillende soortgelijke platforms, zoals Phantom Secure[109] en Exclu[110], werden eveneens ontmanteld, terwijl veel kleinere platforms nog steeds actief zijn en een vrijhaven bieden voor de uitwisseling van criminele informatie. In dit versnipperde landschap is het van essentieel belang dat rechtshandhavingsinstanties in staat zijn criminele communicatiekanalen te identificeren, hun activiteiten te monitoren en te blokkeren, hen te ontmantelen en criminelen voor de rechter te brengen.

---

108 https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf.

109 https://www.fbi.gov/news/stories/phantom-secure-takedown-031618.

110 New strike against encrypted criminal communications with dismantling of Exclu tool | Eurojust | Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken (europa.eu).

Hoewel interceptie via de exploitanten geen optie is bij dit soort malafide aanbieders van communicatie, hebben rechtshandhavingsinstanties nood aan geschikte tactische interceptiecapaciteiten – instrumenten en deskundigheid – om hun gebruikers doelgericht te monitoren, ongeacht de encryptie. Rechtshandhavingsdeskundigen wezen op de aanzienlijke uitdagingen, risico's en beperkingen in verband met de ontwikkeling en het gebruik van dergelijke technieken, die niet schaalbaar zijn en enkel voor de belangrijkste gevallen moeten worden gebruikt. Afhankelijk van hun capaciteiten en het geldende rechtskader gebruiken de nationale autoriteiten verschillende benaderingen, waaronder instrumenten die intern worden ontwikkeld, van derden worden gekocht of als dienst worden geëxploiteerd. Ongeacht welke optie zij gebruiken, zijn de deskundigen het erover eens dat er garanties en waarborgen moeten gelden voor het gebruik van dergelijke instrumenten. Dit kan inhouden dat wordt nagedacht over beter toezicht op en betere evaluatie en certificering van de instrumenten, alsook over een solide kader voor kwetsbaarheidsbeheer, met volledige inachtneming van de procedurele autonomie van de lidstaten in strafzaken en hun exclusieve bevoegdheid op het gebied van nationale veiligheid.

De met het onderzoek belaste autoriteiten worden ook geconfronteerd met juridische uitdagingen, zoals moeilijkheden bij het strafbaar stellen van aanbieders van voornamelijk criminele communicatie- en hostingdiensten (aangezien alle verkeer geëncrypteerd is), wat een noodzakelijke eerste stap is om gerechtelijke of administratieve maatregelen te kunnen nemen. Bovendien moeten de lidstaten sancties kunnen opleggen aan criminele communicatiekanalen om de toegang tot dergelijke diensten in de EU te beperken of te blokkeren en zo hun criminele bedrijfsmodel teniet te doen. Dit zal noodzakelijk blijken wanneer en indien verplichtingen op het vlak van legale interceptie van toepassing zijn op OTT-diensten, om te voorkomen dat criminelen terugkeren naar malafide aanbieders van communicatiediensten.

Ten slotte worden verschillende aspecten van de rechtszaken tegen bijvoorbeeld EncroChat en Sky ECC voor de rechter aangevochten. De vereisten voor het gebruik van in een andere lidstaat onderschepte gegevens als bewijsmateriaal verschillen aanzienlijk binnen de EU, wat leidt tot rechtsonzekerheid bij gelijkaardige operaties die door één lidstaat worden uitgevoerd, met mogelijke gevolgen voor veel andere lidstaten.

MOGELIJKE OPLOSSINGEN

I. Verzoeken om legale interceptie afdwingbaar maken voor alle soorten aanbieders van elektronischecommunicatiediensten

In de EU zijn de capaciteiten op het gebied van legale interceptie beperkt tot traditionele aanbieders van communicatie, terwijl de meeste communicatie momenteel verloopt via niet-traditionele aanbieders van communicatiediensten[111]. Rechtshandhavingsinstanties moeten dezelfde mogelijkheden hebben om legale interceptie uit te voeren bij een persoon van belang, ongeacht of een communicatiedienst al dan niet door de eigenaar van de infrastructuur wordt verleend. Alternatieve oplossingen, zoals het uitvoeren van legale interceptie op NI-ICS en andere communicatiediensten die zich uitsluitend op het niveau van de provider bevinden, waarbij gebruik wordt gemaakt van internationale samenwerkingsinstrumenten om legale interceptie op NI-ICS-aanbieders uit te voeren of waarbij uitgebreid beroep wordt gedaan op tactische interceptie, zijn niet werkbaar[112].

De GHN-deskundigen achten het dan ook van prioritair belang om ervoor te zorgen dat de verplichtingen op het vlak van legale interceptie van beschikbare gegevens op dezelfde wijze van toepassing zijn op traditionele en niet-traditionele aanbieders van communicatiediensten en in gelijke mate afdwingbaar zijn. Door middel van de harmonisatie van die verplichtingen moeten de uitdagingen in verband met de uitvoering van grensoverschrijdende verzoeken kunnen worden overwonnen.

Om dit doel na te streven en geleidelijk toe te werken naar de onderlinge afstemming en harmonisatie van de regels inzake legale interceptie in de EU, stellen de GHN-deskundigen een stapsgewijze aanpak voor: ten eerste moeten de structurerende beginselen op EU-niveau worden overeengekomen (stap 1); vervolgens moet de tenuitvoerlegging van deze beginselen door de Commissie worden ondersteund (stap 2); ten slotte kunnen de beginselen op basis van een nadere beoordeling in een rechtsinstrument worden gecodificeerd (stap 3).

---

111 In het VK werden in 2022 36 miljard sms- en mms-berichten verzonden, terwijl het aantal onlineberichten 1,3 biljoen bedroeg (WhatsAppening in the world of online communications? - Ofcom).

112 Zie deel over uitdagingen.

Stap 1: overeenstemming bereiken over een gemeenschappelijke basis

Ten eerste moet er overeenstemming worden bereikt over de soorten elektronischecommunicatiediensten die kunnen worden onderworpen aan nationale verplichtingen inzake legale interceptie overeenkomstig de e-privacyrichtlijn en de algemene verordening gegevensbescherming.

Ten tweede is er overeenstemming nodig over operationele vereisten op hoog niveau, waarin duidelijk wordt aangegeven wat door de nationale autoriteiten wordt verwacht op het gebied van legale interceptie en wat de bijbehorende waarborgen moeten zijn. LEON[113] werd aangemerkt als een goede basis voor het vaststellen van vereisten op het gebied van rechtshandhaving. Dit document moet vergezeld gaan van vereisten inzake bijvoorbeeld evenredigheid, toezicht en transparantie, waarbij mogelijk een onderscheid wordt gemaakt tussen de regels die van toepassing zijn op inhoudelijke gegevens en die toepasselijk op niet-inhoudelijke gegevens, met volledige inachtneming van cyberbeveiliging, gegevensbescherming en privacy, een en ander zonder encryptie te ondermijnen. De mogelijke oprichting van een ad-hocgroep van deskundigen, onder wie deskundigen op het gebied van cyberaangelegenheden, privacy en rechtshandhaving, zou ervoor kunnen zorgen dat de vereisten waar nodig worden geactualiseerd, eventueel voortbouwend op de werkzaamheden van de Europol-werkgroep voor normalisatie inzake interne veiligheid, die moeten worden voortgezet.

Ten derde moet het begrip territoriale bevoegdheid worden verduidelijkt wat betreft de toepasselijkheid ervan op OTT-diensten, rekening houdend met de uiteenlopende interpretaties door de nationale autoriteiten en, bovenal, door de nationale autoriteiten en de OTT-aanbieders. Zo moeten de regels die van toepassing zijn op gevallen waarin de locatie van het doelwit onzeker is, worden verduidelijkt. Er zijn ook richtsnoeren nodig over wie de rechtmatigheid van een verzoek kan beoordelen, bijvoorbeeld met betrekking tot de rol van dienstverleners in dit verband. Ten slotte is het zeker ook belangrijk dat, hoewel de overgrote meerderheid van de rechterlijke uitspraken tot dusver de wettigheid van procedurele handelingen tegen EncroChat en Sky ECC heeft bevestigd[114], er nog verschillende rechtszaken aanhangig zijn, met mogelijk grote gevolgen voor de veroordeling van prominente criminelen. Bijgevolg is het misschien nodig de toelaatbaarheid van bewijsmateriaal dat is verkregen uit maatregelen inzake tactische interceptie tussen lidstaten, de wederzijdse erkenning van vonnissen en rechterlijke beslissingen en de politiële en justitiële samenwerking in strafzaken te faciliteren.

---

113 LEON (Law Enforcement – Operational Needs for Lawful Access to Communications) is het resultaat van werkzaamheden van Zweedse rechtshandhavingsdiensten in nauwe samenwerking met rechtshandhavingsvertegenwoordigers uit EU-lidstaten, Noord-Amerika en Australië. Het doel ervan is de rechtshandhavingsbehoeften aan rechtmatige toegang tot communicatie-inhoud, inhoudelijke gegevens en abonnee-informatie in kaart te brengen en te beschrijven. Zie *Mededeling van het voorzitterschap van de Raad over operationele behoeften voor rechtmatige toegang tot communicatie ("Law Enforcement Operational Needs for Lawful Access to Communications" – LEON)* (doc. ST 6050/23 van 16 februari 2023).

114 Zie zaken T-1180/23, T-148/24, T-167/24, T-484/24 en T-560/24.

Aanbevelingscluster 7

Om op EU-niveau overeenstemming te bereiken over gemeenschappelijke beginselen voor de legale interceptie van beschikbare gegevens, die van toepassing zijn op alle soorten aanbieders van elektronischecommunicatiediensten, bevelen de deskundigen het volgende aan:

1. *de definitie en het toepassingsgebied van legale interceptie verduidelijken overeenkomstig bestaande EU-handelingen en andere desbetreffende Europese en internationale instrumenten, zoals het Verdrag van Boedapest inzake cybercriminaliteit [aanbeveling 38];*

2. *voortbouwen op het LEON-document om gemeenschappelijke operationele vereisten vast te stellen [aanbeveling 21];*

3. *de nodige waarborgen in kaart brengen [aanbeveling 17, aanbeveling 41];*

4. *het cyberbeveiligingsperspectief zodanig benaderen dat geen enkele maatregel aanbieders ertoe mag verplichten hun ICT-systemen zodanig aan te passen dat de cyberbeveiliging van hun gebruikers negatief wordt beïnvloed [aanbeveling 41];*

5. *het begrip territoriale bevoegdheid voor gegevens verduidelijken om mogelijke wetsconflicten aan te pakken [aanbeveling 39] en de vaststelling bevorderen van minimumvoorschriften op EU-niveau die de toelaatbaarheid mogelijk maken van bewijsmateriaal dat is verkregen uit maatregelen inzake tactische interceptie tussen de lidstaten, voor zover dat nodig is om de wederzijdse erkenning van vonnissen en rechterlijke beslissingen en de politiële en justitiële samenwerking in strafzaken te vergemakkelijken [aanbeveling 42].*

Er moet worden nagedacht over de beste aanpak om gemeenschappelijke beginselen vast te stellen en overeen te komen, zoals vermeld in aanbevelingscluster 7, en om te bepalen welk instrument het meest geschikt is om deze beginselen te delen. Terugkijkend heeft de resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer[115] een belangrijke rol gespeeld bij het vergemakkelijken van de harmonisatie van de oplossingen op het gebied van legale interceptie, aangezien zij een referentie vormde voor door het ETSI ontwikkelde normen inzake legale interceptie. Een soortgelijke aanpak, eventueel door middel van een aanbeveling van de Commissie of de Raad, zou even gunstig kunnen zijn.

[115] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A31996G1104.

Kernactie: de GHN-deskundigen verzoeken de EU om in 2025 te komen met een aanbeveling over realtime toegang tot gegevens

Tijdschema: 2025 *Begroting: nog te bepalen*

- De GHN-deskundigen roepen de Europese Commissie op een aanbeveling te doen waarin het begrip legale interceptie[116] voor aanbieders van elektronischecommunicatiediensten wordt verduidelijkt en de verschillende vereisten worden gespecificeerd die van toepassing kunnen zijn op de legale interceptie van beschikbare niet-inhoudelijke en inhoudelijke gegevens, met volledige inachtneming van cyberbeveiliging, gegevensbescherming en privacy, zonder encryptie te ondermijnen en voortbouwend op gemeenschappelijke operationele vereisten zoals gedefinieerd in het LEON-document.

Stap 2: EU-steun verlenen om een gelijk speelveld te waarborgen en de grensoverschrijdende samenwerking te verbeteren

De in stap 1 uiteengezette gemeenschappelijke beginselen zouden de basis vormen voor technische, juridische en organisatorische harmonisatie op EU-niveau. De omzetting ervan in concrete doelstellingen vereist coördinatie en financiële steun van de Commissie. Dit houdt in dat er een specifiek proces wordt opgezet in het kader waarvan er wordt voortgebouwd op bestaande werkgroepen en er, waar nodig, nieuwe werkgroepen worden opgericht, dat wordt gezorgd voor coördinatie met belanghebbenden, waaronder OTT-aanbieders en vertegenwoordigers van het bedrijfsleven, dat verslag wordt uitgebracht aan de relevante instanties, met name de Raad en het Europees Parlement, en dat transparantie ten opzichte van het publiek wordt gewaarborgd. Het kan ook gaan om de financiering van gerichte studies, rechtstreeks of via relevante partnerschappen, bijvoorbeeld met relevante agentschappen of academische partners.

[116] Beperkt tot interceptie via de exploitanten zoals hierboven gedefinieerd.

Daarnaast benadrukten de GHN-deskundigen dat de efficiëntie van grensoverschrijdende verzoeken om legale interceptie in het huidige kader dringend moet worden verbeterd en tegelijkertijd de hierboven geschetste werkzaamheden moeten worden uitgevoerd. Deze doelstelling omvat:

- het beoordelen van de huidige beperkingen van het EOB[117] en het trachten verbeteren van de operationele efficiëntie;

- het aanpakken van technische en organisatorische beperkingen in verband met de grensoverschrijdende uitwisseling van bewijsmateriaal dat is verzameld door middel van legale interceptie, waarvoor op zijn beurt verdere werkzaamheden nodig zouden zijn op het gebied van:

    - het in kaart brengen van het probleem (wat zijn de beperkingen, welke lidstaten worden ermee geconfronteerd, enz.);

    - de standaardisering van gegevensstructuren, vertrouwensmechanismen en gegevensfiltering om te voorkomen dat gegevens worden doorgegeven die niet relevant zijn en om de gegevensbeschermingsbeginselen van doelbinding, evenredigheid en gegevensminimalisering in acht te nemen;

    - de opzet en capaciteit van grensoverschrijdende transmissiemiddelen;

    - het in kaart brengen van de bijbehorende financieringsregelingen;

- het faciliteren van grensoverschrijdende verzoeken om legale interceptie door centrale contactpunten aan te wijzen en op te leiden, in coördinatie met de bredere werkzaamheden op het gebied van centrale contactpunten en toegang tot digitaal bewijsmateriaal, met een prominente rol voor het Sirius-project;

- in voorkomend geval, het bevorderen van bilaterale overeenkomsten tussen de lidstaten en de VS als voorwaarde voor het faciliteren van rechtstreekse verzoeken van nationale autoriteiten aan reguliere aanbieders van OTT-diensten, aangezien het toepassingsgebied van de overeenkomst tussen de EU en de VS inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal waarover momenteel wordt onderhandeld, volgens de onderhandelingsrichtsnoeren geen betrekking heeft op legale interceptie, wat betekent dat specifieke overeenkomsten nodig zijn om wetsconflicten aan te pakken.

---

[117] In het kader van Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken wordt verwezen naar “telecommunicatie”; hoewel de meeste lidstaten dit begrip ruimer hebben geïnterpreteerd, zou, in overeenstemming met de actualisering van het EECC, de mogelijke noodzaak om het EOB in dat opzicht te wijzigen, kunnen worden overwogen en verder beoordeeld.

Tot slot vroegen de deskundigen na te denken over manieren om de afschrikkende maatregelen van de nationale autoriteiten tegen niet-coöperatieve elektronischecommunicatiediensten te verbeteren. De deskundigen verzochten met name om de haalbaarheid en evenredigheid van mogelijke technische oplossingen te beoordelen.

Aanbevelingscluster 8

Om ervoor te zorgen dat een breed scala aan aanbieders van elektronischecommunicatiediensten, met inbegrip van aanbieders van OTT-diensten, ingaan op verzoeken om legale interceptie zoals bepaald in de nationale wetgeving, bevelen de deskundigen aan:

1. *de tenuitvoerlegging van de in aanbeveling 1.1 vastgelegde beginselen te ondersteunen door middel van coördinatie en financiering;*

2. *na te gaan hoe het EOB efficiënte grensoverschrijdende verzoeken om legale interceptie beter kan ondersteunen, bijvoorbeeld door de rechtszekerheid te verbeteren, de termijnen voor het beantwoorden van bevelen te verkorten en een uniform gebruik van het EOB te bevorderen [aanbeveling 40];*

3. *mechanismen (interoperabiliteit en cyberbeveiliging) en infrastructuur (bandbreedte en schaalbaarheid) tot stand te brengen die compatibel zijn met de grensoverschrijdende overdracht in real time van grote datasets [aanbeveling 9];*

4. *de aanwijzing te bevorderen van centrale contactpunten in de EU die moeten omgaan met verzoeken van en instaan voor de contacten met overheidsinstanties, teneinde de handhaving van de verplichtingen inzake legale interceptie te vergemakkelijken en mechanismen in te stellen voor een efficiënte aanpak van grensoverschrijdende verzoeken [aanbevelingen 19 en 36];*

5. *de ontwikkeling te stimuleren van bilaterale overeenkomsten met derde landen, met name de Verenigde Staten, inzake toegang in realtime tot gegevens [aanbeveling 38.4].*

Een aantal activiteiten zou de doeltreffende uitvoering van een EU-aanbeveling inzake legale interceptie kunnen ondersteunen.

Kernactie: de GHN-deskundigen verzoeken de Commissie om de uitvoering van een EU-aanbeveling inzake legale interceptie vergezeld te doen gaan van passende coördinatie en financiering

- De GHN-deskundigen verzoeken de Commissie een duidelijk plan voor te stellen ter ondersteuning van de uitvoering van een EU-aanbeveling inzake legale interceptie, ook vanuit het oogpunt van financiële planning.

Stap 3: beoordelen of een rechtsinstrument inzake legale interceptie mogelijk is

Enkel coördinatie kan ontoereikend blijken om het vereiste niveau van harmonisatie te bereiken, ook al gaat dit vergezeld van maatregelen om de bestaande rechtsinstrumenten efficiënter te maken. Een nieuwe reeks regels kan nodig zijn om de afdwingbaarheid van verzoeken en rechtszekerheid te waarborgen, wetsconflicten weg te nemen en de administratieve lasten in verband met nalevings- en wettigheidscontroles te verminderen. Bovendien brengen de verschillen tussen de regels inzake legale interceptie in de EU belastende vereisten met zich mee voor gereguleerde entiteiten zoals aanbieders van OTT-diensten, waardoor belemmeringen voor de markttoegang van aanbieders van communicatiediensten kunnen ontstaan[118]. In dat verband zouden geharmoniseerde EU-regels inzake legale interceptie van beschikbare gegevens bijdragen tot de opbouw van de toekomstige digitale infrastructuur van Europa, waarbij voorkeur wordt gegeven aan een model in het kader waarvan telecommunicatie-infrastructuur een potentieel continentale dekking biedt[119].

De overgang naar internetcommunicatie is een sterke stimulans om geharmoniseerde toegangsregels op EU-niveau vast te stellen. De aanvaardbaarheid, de haalbaarheid en de gevolgen voor het bedrijfsleven, de cyberbeveiliging en de veiligheid van een rechtsinstrument moeten echter zorgvuldig worden beoordeeld, rekening houdend met de huidige verschillen tussen de rechtsstelsels van de lidstaten op het vlak van legale interceptie. De GHN-deskundigen verklaarden dat een mogelijk instrument: i) in overeenstemming moet zijn met de beginselen van aanbeveling 1.1; ii) ten volle rekening moet houden met het grondrechtenperspectief en de soevereiniteit van landen op het vlak van strafzaken en nationale veiligheid; en iii) inspiratie moet putten uit het werk dat is verricht met betrekking tot het pakket elektronisch bewijsmateriaal.

De GHN-deskundigen waren het erover eens dat elk initiatief om regels inzake legale interceptie voor alle soorten elektronischecommunicatiediensten te bevorderen of op te leggen, vergezeld moet gaan van een duidelijk en afdwingbaar kader voor het nemen van maatregelen tegen aanbieders van communicatiediensten die illegaal opereren en/of elke vorm van samenwerking met rechtshandhavingsinstanties weigeren. Zonder dergelijk kader zouden de regels worden ondermijnd en zouden criminele actoren hun communicatie massaal naar niet-conforme aanbieders verplaatsen. Bij elk toekomstig EU-initiatief in dit verband moet rekening worden gehouden met het verschil tussen aanbieders van OTT-diensten die hun wettelijke verplichtingen niet nakomen en elektronischecommunicatiediensten die bewust diensten voorstellen die zijn toegesneden op criminele activiteiten. Daarnaast moet bij elk initiatief ook rekening worden gehouden met het EU-acquis, en met name de digitaledienstenverordening.

---

118 Zie “Lawful interception – A market access barrier in the European Union”, Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

119 Witboek - How to master Europe’s digital infrastructure needs? | Shaping Europe’s digital future (europa.eu).

Dergelijk initiatief kan administratieve of gerechtelijke maatregelen omvatten. De GHN-deskundigen vroegen grondig na te denken over deze kwestie, en daarbij zowel rekening te houden met de problemen op het gebied van grondrechten en cyberbeveiliging als met de complexe technologische uitdagingen.

Aanbevelingscluster 9

De deskundigen bevelen aan om op basis van een nadere analyse en een effectbeoordeling ***een EU-instrument voor legale interceptie (bestaande uit "zachte" of bindende rechtsinstrumenten) voor rechtshandhavingsdoeleinden te ontwerpen*** *waarmee afdwingbare verplichtingen worden opgelegd aan aanbieders van elektronischecommunicatiediensten in de EU. Zij bevelen aan dat dit potentiële instrument: [aanbeveling 38]*

1. *de beginselen volgt die zijn overeengekomen in aanbevelingscluster 7;*
2. *technologieneutraal is [aanbeveling 21];*
3. *de harmonisatie op EU-niveau bevordert van strafrechtelijke maatregelen, met inbegrip van gevangenisstraffen, tegen niet-coöperatieve elektronischecommunicatiediensten om samenwerking af te dwingen [aanbeveling 34];*
4. *ten volle rekening houdt met het grondrechtenperspectief en de soevereiniteit van landen op het vlak van strafzaken en nationale veiligheid [aanbeveling 38];*
5. *inspiratie put uit het werk dat is verricht in het kader van de vaststelling van regels inzake elektronisch bewijsmateriaal [aanbeveling 38, punt iv)];*
6. *dienstverleners verplicht bepaalde functies in hun diensten aan of uit te zetten om informatie te verkrijgen na ontvangst van een bevel (bv. het opslaan van de geolocatie van een specifieke gebruiker nadat er een rechtmatig verzoek tegen hem/haar is ingediend) [aanbeveling 32];*
7. *mechanismen omvat om ervoor te zorgen dat de lidstaten sancties kunnen opleggen aan niet-coöperatieve elektronischecommunicatiediensten (administratieve of strafrechtelijke maatregelen, afhankelijk van de vraag of een aanbieder louter niet-coöperatief is of een dienst van criminele aard aanbiedt), in overeenstemming met en mogelijk voortbouwend op de regels van de digitaledienstenverordening, en dat dergelijke sancties afschrikkend werken ten aanzien van die entiteiten [aanbeveling 33].*

Handhaving van de beginselen van een EU-aanbeveling inzake legale interceptie zou een belangrijke stap betekenen in de richting van meer geharmoniseerde en meer afdwingbare regels inzake legale interceptie. Er kan echter nog steeds een rechtsinstrument nodig zijn om de rechtszekerheid te verbeteren, ervoor te zorgen dat alle betrokken elektronischecommunicatiediensten bij de uitvoering van legale interceptie over de nodige waarborgen beschikken, en ervoor te zorgen dat elektronischecommunicatiediensten die niet bereid zijn de door de lidstaten vastgestelde regels te handhaven, daartoe verplicht worden.

Kernactie: de GHN-deskundigen verzoeken de Commissie de verdere ontwikkeling van het wetgevingskader inzake legale interceptie voor rechtshandhavingsdoeleinden te beoordelen

- De GHN-deskundigen verzoeken de Europese Commissie om, voorafgaand aan een mogelijke effectbeoordeling, te beoordelen of een EU-rechtsinstrument betreffende legale interceptie mogelijk is, voortbouwend op het werk dat is verricht ter voorbereiding van de EU-verordening en -richtlijn inzake elektronisch bewijsmateriaal, en zich te richten op het in kaart brengen van mogelijke technologieneutrale oplossingen.

II. Technologische uitdagingen aanpakken

Veel uitdagingen waarmee rechtshandhavingsinstanties worden geconfronteerd met betrekking tot de toegang tot gegevens, vloeien voort uit hoe moeilijk het voor hen is om te anticiperen op technologische ontwikkelingen en zich daaraan aan te passen. In tegenstelling tot actoren in andere sectoren, zoals defensie of ruimtevaart, beschikken rechtshandhavingsinstanties namelijk niet over de middelen of de nauwe banden met de industrie die nodig zijn om dit te doen, en zijn zij er ook niet mee vertrouwd dit te hoeven doen. In veel gevallen proberen actoren op het gebied van interne veiligheid technologische lacunes op reactieve wijze op te vullen of, vaker nog, proberen zij in hun behoeften te voorzien met beschikbare en betaalbare kant-en-klare technologie. Om een verschuiving van een reactieve naar een proactievere aanpak in de hand te werken, moeten technologische uitdagingen op gestructureerde, toekomstgerichte en multidisciplinaire wijze worden aangepakt, met twee hoofdprioriteiten: vanuit het oogpunt van de nationale autoriteiten is het van essentieel belang ervoor te zorgen dat rechtshandhavingsinstanties toegang hebben tot de passende capaciteiten om beschikbare gegevens in doorvoer te verkrijgen en te verwerken; voor exploitanten en technologieaanbieders is het van essentieel belang dat zij hun verplichtingen op het gebied van toegang tot gegevens, privacy en cyberbeveiliging kunnen nakomen en dat hun belangen worden beschermd.

Deskundigen stellen daarom voor te anticiperen op technologische uitdagingen door middel van een alomvattend en toekomstgericht beleid, gebaseerd op een **technologieroutekaart voor rechtmatige toegang**, waarmee doelstellingen worden vastgesteld en activiteiten worden opgezet met bijbehorende financiering om die doelstellingen te verwezenlijken.

Wat capaciteitsopbouw betreft zijn de uitdagingen weliswaar verschillend, maar de door de deskundigen voorgestelde aanpak is vaak vergelijkbaar voor digitaal forensisch onderzoek, gegevensbewaring en legale interceptie[120] en bouwt voort op dezelfde aanbevelingen, met een sterke vraag naar doelgerichte planning om financieringsmogelijkheden te sturen, waarbij actoren uit het bedrijfsleven en belangrijke belanghebbenden, zoals de Europese innovatiehub voor interne veiligheid, nauwer worden betrokken.

Rechtshandhavingsdeskundigen legden echter de nadruk op twee elementen die specifiek zijn voor legale interceptie.

- Een intensiever gebruik van metagegevens – bv. locatiegegevens, gespreksopnames en koppen van e-mails – kan extra aanwijzingen opleveren in het kader van onderzoeken. **Naarmate steeds meer apparaten op het internet worden aangesloten, zal het volume aan gegenereerde gegevens toenemen, waardoor er meer mogelijkheden zullen zijn om gedragspatronen in kaart te brengen.** De deskundigen riepen op tot meer onderzoek, innovatie en concrete toepassingen met betrekking tot **een ruimer gebruik van metagegevens**, bijvoorbeeld via AI, als een manier om de gevolgen van het gebrek aan toegang tot inhoudelijke gegevens te matigen. Tegelijkertijd wezen zij op de risico's voor de privacy in verband met het op grote schaal verwerken van persoonlijke metagegevens door AI-toepassingen, die moeten worden afgewogen tegen een gericht gebruik van inhoudelijke gegevens. Rechtshandhavingsdeskundigen laten er echter geen twijfel over bestaan dat metagegevens alleen de bewijskracht van communicatie-inhoud voor het aantonen van opzet niet volledig kunnen vervangen.

- Wanneer criminelen gebruikmaken van specifieke communicatieplatforms met eind-tot-eindencryptie, moeten rechtshandhavingsinstanties gebruikmaken van tactische oplossingen op basis van de benutting van **kwetsbaarheden** om toegang te krijgen tot de communicatie van verdachten. Een aantal rechtshandhavingsinstanties werkt al binnen een wettelijk kader dat interceptie aan communicatie-eindpunten mogelijk maakt en beschikt daartoe over de nodige technologie, en er is ruimte voor verdere vooruitgang op dit gebied. Dit kan inhouden dat steun wordt verleend aan de ontwikkeling van in de EU vervaardigde instrumenten en dat de rechtshandhavingsinstanties deze kunnen aanschaffen en gebruiken binnen het bestaande rechtskader.

  Rechtshandhavingsdeskundigen merkten echter op dat deze methode niet mag uitgroeien tot een van de voornaamste middelen voor het verzamelen van bewijsmateriaal, aangezien tactische interceptie noch schaalbaar noch zonder problemen is. Zo kunnen zich bevoegdheidskwesties voordoen op basis van de locatie van het doelwit. Bovendien is het benutten van kwetsbaarheden die niet openbaar kunnen worden gemaakt, onvermijdelijk in strijd met de kernbeginselen inzake cyberbeveiliging.

[120] Nader uitgewerkt in het hoofdstuk over digitaal forensisch onderzoek.

Wat rechtmatige toegang door ontwerp betreft, stelden rechtshandhavingsdeskundigen een voorzichtige aanpak voor, aangezien van actoren uit het bedrijfsleven niet mag worden gevraagd een systeem te integreren dat de encryptie op algemene of systemische wijze voor alle gebruikers van een dienst kan verzwakken; rechtmatige toegang tot communicatie moet doelgericht blijven, en per geval plaatsvinden. Zij waren het eens over de relevantie van de algemene doelstelling, maar benadrukten dat stap per stap vooruitgang moet worden geboekt en dat alle relevante categorieën belanghebbenden, met inbegrip van deskundigen op het gebied van technologie, cyberbeveiliging en privacy, moeten worden betrokken, rekening houdend met de potentiële risico's en de gevoeligheid van het publieke debat. Zij raadden met name ten zeerste aan een empirisch onderbouwde aanpak te volgen en zorgvuldig de beschikbaarheid te beoordelen van technische oplossingen die de cyberbeveiliging van communicatie niet verzwakken of negatieve gevolgen hebben voor de cyberbeveiliging van exploitanten.

Aanbevelingscluster 10

Om de technologische uitdagingen van legale interceptie aan te pakken, bevelen de deskundigen aan ***een technologieroutekaart voor rechtmatige toegang***[121] *te ontwikkelen, die met name:*

1. *deskundigen op het gebied van technologie, cyberbeveiliging, privacy, normalisatie en beveiliging samenbrengt en zorgt voor adequate coördinatie, eventueel door middel van een permanente structuur [aanbeveling 22];*
2. *onderzoek naar en de ontwikkeling en toepassing van instrumenten voor de verwerving van en toegang tot gegevens bevordert, met inbegrip van decryptiecapaciteit, alsook op AI gebaseerde capaciteiten voor gegevensanalyse*[122] *[aanbeveling 4];*
3. *een gecoördineerde aanpak van normalisatie bevordert, waarbij in voorkomend geval rekening wordt gehouden met de behoeften aan rechtmatige toegang tot gegevens, en tevens [aanbevelingen 15, 16 en 20]:*
    a. *de betrokkenheid van beroepsbeoefenaars uit alle relevante geledingen bij relevante normalisatiegroepen bevordert;*
    b. *toekomstige initiatieven vergezeld doet gaan van adequate normalisatiemaatregelen (ter bevordering van een technologieneutrale aanpak);*
    c. *betrekking heeft op communicatietechnologieën in het algemeen, IoT (met inbegrip van bijvoorbeeld verbonden auto's) en elke vorm van connectiviteit (met inbegrip van bijvoorbeeld satellietcommunicatie);*
4. *de EU-coördinatie met het bedrijfsleven verbetert om situaties aan te pakken waarin technologische oplossingen bestaan maar niet worden toegepast; in dergelijke gevallen*[123] *zijn duidelijke richtsnoeren en een op EU-niveau gefaciliteerde dialoog nodig [aanbeveling 24];*
5. *rechtmatige toegang door ontwerp implementeert voor alle desbetreffende technologieën, in overeenstemming met de door de rechtshandhavingsinstanties geuite behoeften, waarbij tegelijkertijd een sterke beveiliging en cyberbeveiliging worden verzekerd en ervoor wordt gezorgd dat de wettelijke verplichtingen inzake rechtmatige toegang worden nageleefd [aanbeveling 22];*
6. *de uitdagingen op het gebied van encryptie grondig aanpakt door:*
    a. *ervoor te zorgen dat eventuele nieuwe verplichtingen en/of normen niet rechtstreeks of onrechtstreeks leiden tot verplichtingen voor aanbieders om de veiligheid van de communicatie te verminderen door eind-tot-eindencryptie in het algemeen te ondermijnen of te verzwakken [aanbeveling 23];*
    b. *ervoor te zorgen dat rechtmatige toegang door ontwerp geen negatieve gevolgen heeft voor de beveiligingsmaturiteit van de betrokken hardware- of softwarearchitecturen [aanbeveling 23];*
    c. *op een gecoördineerde wijze en met steun van EU-financiering te werken aan een methode om gerichte rechtmatige toegang te ontwikkelen, te hanteren en te gebruiken om om te gaan met gevallen waarin toegang tot gegevens niet mogelijk is middels samenwerking met elektronischecommunicatiediensten [aanbeveling 10].*

---

[121] De technologieroutekaart moet de drie werkterreinen bestrijken: digitaal forensisch onderzoek, gegevensbewaring en legale interceptie.

[122] Deze aanbeveling is ook van toepassing op de toegang tot gegevens op een apparaat (zie deel over digitaal forensisch onderzoek), maar de praktijkvoorbeelden verschillen enigszins.

[123] Bijvoorbeeld wanneer home-routingovereenkomsten of een specifieke implementatie van RCS geen legale interceptie toelaten.

Hoewel sommige door de GHN-deskundigen voorgestelde initiatieven reeds gedeeltelijk bestaan, is er een grote behoefte aan een betere structurering van de technologieroutekaart wat betreft het technologisch beleid op middellange en lange termijn inzake rechtmatige toegang, met gerichte doelstellingen en een bijbehorend monitoringinstrument. Deze aanpak moet niet alleen betrekking hebben op de toegang tot gegevens in doorvoer, maar ook op digitaal forensisch onderzoek en gegevensbewaring.

De technologieroutekaart moet toekomstgericht en afdwingbaar zijn, gericht zijn op prioritaire onderwerpen en verankerd zijn in de digitale strategie van de EU. Ook moeten alle relevante categorieën belanghebbenden, met name EU-instellingen, -organen en -agentschappen, nationale autoriteiten, academici op alle relevante gebieden, het bedrijfsleven en ngo's, hier nauw bij worden betrokken, en moet er een duidelijk bestuur zijn.

Kernactie: de GHN-deskundigen dringen er bij de Commissie op aan een technologieroutekaart voor de toegang tot gegevens voor te stellen en uit te voeren

- De GHN-deskundigen verzoeken de Europese Commissie een technologieroutekaart op te stellen en uit te voeren die gericht is op uitdagingen op het gebied van encryptie, waarin alle relevante aspecten aan bod komen, onder meer op het vlak van technologie, de markt, cyberbeveiliging, de grondrechten, normalisatie, rechtshandhaving en onderzoek. Deze technologieroutekaart moet in 2025 beschikbaar zijn en moet voortbouwen op alle relevante deskundigheid van de lidstaten en de EU-instellingen, -organen en -agentschappen, onder meer op het gebied van cyberbeveiliging, gegevensbescherming en privacy.