Advies 23/2018 inzake de voorstellen van de Commissie betreffende de Europese bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal in strafzaken (artikel 70, lid 1, onder b))

Uitgebracht op 26 september 2018

Inhoud

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder b), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG,

BRENGT HET VOLGENDE ADVIES UIT:

Inleiding

De Commissie heeft in april 2018 een voorstel voor een verordening ingediend betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken alsmede een voorstel voor een richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures. Beide voorstellen COM(2018) 225 final en COM(2018) 226 final vullen elkaar aan. Het algemene doel dat de Commissie nastreeft is de samenwerking tussen de autoriteiten van de lidstaten en dienstverleners, ook in derde landen gevestigde dienstverleners, te verbeteren en oplossingen voor te stellen voor het probleem van de bepaling en handhaving van de rechtsmacht in de cyberruimte.

Terwijl in de ontwerpverordening de regels en procedures voor de uitvaardiging, het gebruik en de tenuitvoerlegging van bewarings- en verstrekkingsbevelen ten aanzien van verleners van elektronische-communicatiediensten zijn vastgelegd, voorziet de ontwerprichtlijn in minimumregels voor de aanwijzing van een wettelijke vertegenwoordiger voor dienstverleners die niet in de EU zijn gevestigd.

Voordat de Commissie een ontwerpvoorstel indiende, wees de Groep artikel 29 er in november 2017[1] op dat eventuele wetgevingsvoorstellen met name volledig in overeenstemming moesten zijn met het EU-acquis inzake gegevensbescherming, maar ook met het EU-recht en de rechtspraak in het algemeen.

In het bijzonder heeft de Groep artikel 29 gewaarschuwd voor beperkingen van de rechten op gegevensbescherming en privacy met betrekking tot door aanbieders van telecomdiensten en diensten van de informatiemaatschappij verwerkte gegevens, met name bij een verdere verwerking door rechtshandhavingsinstanties; gewezen op het belang om de consistentie tussen EU-instrumenten en het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit en de Europese richtlijn betreffende het Europees onderzoeksbevel in strafzaken (de EOB-richtlijn) te waarborgen; en geadviseerd duidelijkheid te verschaffen over de verschillende procedurele voorschriften voor toegang tot elektronisch bewijs op nationaal en EU-niveau om ervoor te zorgen dat autoriteiten met het nieuwe instrument geen nieuwe bevoegdheden in handen krijgen waarover zij intern niet zouden kunnen beschikken. Afgezien van deze algemene opmerkingen is de Groep artikel 29 ook ingegaan op de destijds door de Commissie overwogen wetgevingsopties betreffende de betrokken categorieën van gegevens en de waarborgen voor toegang hiertoe, de mogelijkheid verstrekkingsbevelen/verzoeken

[1] Zie verklaring Groep artikel 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

in te dienen om dienstverleners te dwingen gegevens te verstrekken van buiten de EU, en de materiële en procedurele voorwaarden voor waarborgen voor directe toegang tot gegevens.

Het Europees Comité voor gegevensbescherming (EDPB) wil aan de hand van de concrete voorstellen die op het gebied van elektronisch bewijs gedaan zijn, vanuit het oogpunt van gegevensbescherming dieper ingaan op de voorgestelde rechtsinstrumenten.

1. Rechtsgrondslag van het voorstel voor een verordening (artikel 82 VWEU)

Artikel 82, lid 1, VWEU betreffende de justitiële samenwerking in strafzaken is aangemerkt als rechtsgrondslag voor de ontwerpverordening inzake elektronisch bewijsmateriaal. Hierin wordt het volgende bepaald:

> "1. De justitiële samenwerking in strafzaken in de Unie berust op het beginsel van de wederzijdse erkenning van rechterlijke uitspraken en beslissingen en omvat de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten op de in lid 2 en in artikel 83 genoemde gebieden.
>
> Het Europees Parlement en de Raad stellen, volgens de gewone wetgevingsprocedure, maatregelen vast die ertoe strekken:
>
> a) regels en procedures vast te leggen waarmee alle soorten vonnissen en rechterlijke beslissingen overal in de Unie erkend worden;
>
> b) jurisdictiegeschillen tussen de lidstaten te voorkomen en op te lossen;
>
> c) de opleiding van magistraten en justitieel personeel te ondersteunen;
>
> d) in het kader van strafvervolging en tenuitvoerlegging van beslissingen de samenwerking tussen de justitiële of gelijkwaardige autoriteiten van de lidstaten te bevorderen.″

Zoals de Commissie in de effectbeoordeling bij de voorstellen heeft benadrukt, "In artikel 82, lid 1, wordt bepaald dat de justitiële samenwerking in strafzaken berust op het beginsel van de wederzijdse erkenning. Deze rechtsgrondslag zou wetgeving mogelijk maken op het gebied van directe samenwerking met dienstverleners, waarbij de autoriteit in de uitvaardigende lidstaat zich direct zou richten tot een entiteit (de dienstverlener) in de tenuitvoerleggingsstaat en deze zelfs verplichtingen zou kunnen opleggen. Dit zou een nieuwe dimensie toevoegen aan de wederzijdse erkenning, die verder reikt dan de traditionele justitiële samenwerking binnen de Unie, die tot dusver gebaseerd is op procedures waarbij twee justitiële autoriteiten betrokken zijn, één in de uitvaardigende lidstaat en één in de tenuitvoerleggingsstaat." (nadruk toegevoegd)

Aangezien de toepassing van deze rechtsgrondslag in het kader van directe verzoeken tussen overheidsinstanties en particuliere partijen nieuw is, betreurt de EDPB dat de Commissie geen verdere analyse of beoordeling heeft verstrekt.

Zoals ook de werkgroep in zijn eerdere verklaring al heeft benadrukt, houdt de EDPB vast aan zijn twijfels over de gepastheid van deze rechtsgrondslag, wat ook onderschreven wordt in de analyse van het HvJ-EU en zijn advocaat-generaal in zijn advies 1/15. Een van de ontwikkelingen rondom de vaststelling van de gepastheid van artikel 82 als rechtsgrondslag voor de ontwerp-PNR-overeenkomst tussen de EU en Canada, is de constatering van het Hof dat de bevoegde Canadese autoriteit "*noch*

een justitiële, noch een gelijkwaardige autoriteit" is[2]. Wat de voorstellen op het gebied van elektronisch bewijs betreft, is een van de belangrijkste doelen, zoals de Commissie verklaarde, het voorkomen dat justitiële samenwerking "te omslachtig" wordt. Bijgevolg is het voorstel gebaseerd op het principe dat samenwerking moet plaatsvinden tussen een autoriteit en een dienstverlener en niet tussen twee autoriteiten. De aanvankelijke procedure plaatst particuliere entiteiten in de positie van ontvangende partij die op verzoeken van justitiële autoriteiten kan reageren.

Volgens de EDPB zou het binnen het proces van de tenuitvoerlegging van verstrekkings- of bewaringsbevelen zo kunnen zijn dat een ontvangende autoriteit optreedt indien de ontvangende dienstverlener niet aan zijn verplichtingen voldoet en achteraf een tenuitvoerlegging van het bevel nodig is. Aangezien het hoofddoel van de procedure juist is geen ontvangende autoriteit erbij te betrekken, betwijfelt de EDPB of deze bijkomende procedure de toepassing van artikel 82 als enige rechtsgrondslag voor het instrument rechtvaardigt.

Daarom stelt de EDPB zich op het standpunt dat artikel 82 alleen als rechtsgrondslag kan dienen als de samenwerking grotendeels plaatsvindt tussen twee justitiële autoriteiten en dat voor deze vorm van samenwerking een andere rechtsgrondslag moet worden gezocht.

2. De noodzaak van elektronisch bewijs versus rechtshulpverdragen en EOB

Volgens de EDPB zet de Commissie zich ervoor in belemmeringen voor strafrechtelijke onderzoeken, met name wat betreft de toegang tot elektronisch bewijs, opnieuw te bekijken. De Commissie schetst in haar toelichting het kader van het voorstel en benadrukt het vluchtige karakter en de internationale dimensie van elektronisch bewijsmateriaal, alsook de noodzaak om het samenwerkingsmechanisme aan te passen aan het digitale tijdperk. Voorstellen voor een verordening en een richtlijn voor de overdracht van en de toegang tot elektronisch bewijs hebben niet als doel bestaande samenwerkingsinstrumenten op het gebied van strafzaken, zoals het Verdrag van Boedapest, het verdrag inzake wederzijdse rechtshulp (MLAT) en het Europees onderzoeksbevel in strafzaken (de EOB-richtlijn), te vervangen. Volgens de Commissie beogen de voorstellen inzake elektronisch bewijsmateriaal de justitiële samenwerking in strafzaken tussen autoriteiten en dienstverleners in de Unie en met derde landen, de Verenigde Staten van Amerika in het bijzonder, te verbeteren.

Aangezien deze nieuwe aanvullende instrumenten speciaal gericht zijn op de toegang tot en de overdracht van elektronisch bewijs, zal de EDPB de toegevoegde waarde van de instrumenten in het licht van de EOB-richtlijn en het rechtshulpverdrag beoordelen.

a) De noodzaak van elektronisch bewijs versus de waarborgen van rechtshulpverdragen en EOB

Het belangrijkste argument van de Commissie ten gunste van de voorstellen op het gebied van elektronisch bewijsmateriaal, is het proces inzake het veiligstellen en verkrijgen van elektronisch bewijs dat is opgeslagen en/of wordt bewaard door dienstverleners die binnen een andere jurisdictie zijn gevestigd, sneller te laten verlopen.

[2] Zie punt 103 van advies 1/15 en punt 108 van de conclusie van de advocaat-generaal in deze zaak.

De EDPB betreurt echter dat de noodzaak van nieuwe instrumenten om de toegang tot elektronisch bewijs te regelen, niet in de effectbeoordeling is aangetoond. In de voorstellen ontbreekt inderdaad een onderbouwing waaruit blijkt dat geen andere, minder ingrijpende middelen voorhanden waren om het doel van het voorstel inzake elektronisch bewijsmateriaal te realiseren, terwijl alternatieve oplossingen konden worden overwogen. Er is bijvoorbeeld niet gekeken naar de mogelijkheid om de EOB-richtlijn aan te passen of te verbeteren, waarmee bovendien voldaan zou zijn aan de specifieke vereiste onder de EOB-richtlijn om te evalueren of de tekst voor 21 mei 2019 zou moeten worden aangepast[3]. Een andere mogelijkheid zou zijn geweest om door middel van bewaringsbevelen gegevens te bevriezen, mits een formeel verzoek op basis van een rechtshulpverdrag zou zijn uitgevaardigd. Door deze mogelijkheden hadden de waarborgen die deze instrumenten bieden, gehandhaafd kunnen worden, zonder dat de gevraagde persoonsgegevens zouden worden gewist.

Volgens de EDPB worden in de EOB-richtlijn langere termijnen gehanteerd dan in het voorstel inzake elektronisch bewijsmateriaal. De uitvoerende autoriteit heeft inderdaad dertig dagen de tijd om een beslissing over de erkenning van het verzoek te nemen[4] en moet de maatregel dan binnen negentig dagen uitvoeren[5]. De EDPB is van oordeel dat een beslistermijn van dertig dagen voor de uitvoerende autoriteiten in het EOB een cruciale waarborg is die hun in staat stelt te beoordelen of het uitvoeringsverzoek gegrond is en aan alle voorwaarden voor het uitvaardigen en toezenden van een EOB voldoet[6].

De EDPB is bezorgd dat de in de voorstellen inzake elektronisch bewijsmateriaal voorgelegde termijn van tien dagen voor de uitvaardiging van het Europees verstrekkingsbevel (CEV), onvoldoende is om te beoordelen of het CEV aan alle criteria voldoet en in alle opzichten goed is.

Daarom adviseert de EDPB de adressaat van het CEV meer tijd te bieden om vast te stellen of het bevel al dan niet moet worden uitgevoerd.

Volgens de EDPB is er in het geval van een Europees bewaringsbevel (CEB) geen garantie dat gegevens niet langer bewaard zullen worden dan nodig is om de gegevens te kunnen verstrekken. Gegevens mogen namelijk langer dan zestig dagen bewaard worden, aangezien aan de uitvaardigende autoriteit geen termijn wordt gesteld waarbinnen de adressaat op de hoogte moet worden gesteld van het besluit om een bevel tot verstrekking achterwege te laten of in te trekken. Daarom adviseert de EDPB in ieder geval om aan de uitvaardigende autoriteit een termijn te stellen voor het achterwege laten of intrekken van het bevel tot verstrekking, zodat voldaan kan worden aan het beginsel van minimale gegevensverwerking dat is vastgelegd in de AVG[7].

Tot slot stelt de EDPB dat in de EOB-richtlijn is vastgelegd dat bewijsmateriaal door de uitvaardigende staat aan de uitvoerende staat moet worden teruggegeven[8]. In het voorstel voor een verordening inzake elektronisch bewijsmateriaal wordt echter niet over deze mogelijkheid gesproken. Het is onduidelijk wat er met het elektronische bewijs gebeurt nadat het is overgedragen aan de uitvaardigende autoriteit.

Daarom adviseert de EDPB dat het voorstel voor een verordening meer duidelijkheid moet verschaffen over het gebruik van elektronisch bewijs nadat dit is overgedragen aan de uitvaardigende autoriteit,

[3] Zie artikel 37 van de EOB-richtlijn.
[4] Artikel 12, lid 3, EOB-richtlijn.
[5] Artikel 12, lid 4, EOB-richtlijn.
[6] Artikel 6 van de EOB-richtlijn.
[7] Artikel 5, lid 1, onder c), AVG.
[8] Artikel 13, leden 3 en 4, EOB-richtlijn.

zodat aan de AVG, het transparantiebeginsel[9] en het specificiteitsbeginsel uit de rechtshulpverdragen kan worden voldaan.

b) Afstand van het beginsel van de dubbele strafbaarheid

De EDPB erkent dat wederzijdse erkenning afhankelijk is van de toepassing van het beginsel van de dubbele strafbaarheid, waardoor de lidstaten de mogelijkheid hebben hun soevereiniteit te bewaren. Het beginsel van de dubbele strafbaarheid wordt echter steeds vaker gezien als een obstakel voor een soepele justitiële samenwerking. De EU-lidstaten zijn steeds vaker bereid tot samenwerking, zelfs als onderzoeksmaatregelen betrekking hebben op handelingen die op grond van hun nationale wetgeving niet als strafbaar feit worden aangemerkt. De EDPB wijst er echter op dat het beginsel van de dubbele strafbaarheid bedoeld is als aanvullende waarborg, die ervoor moet zorgen dat een staat geen hulp van een andere staat kan krijgen bij het opleggen van een strafrechtelijke sanctie die in de wetgeving van de andere staat niet bestaat. Daardoor zou bijvoorbeeld voorkomen worden dat een staat van een andere staat geen hulp kan verlangen bij de gevangenzetting van iemand wegens diens politieke opvattingen als deze opvattingen niet strafbaar zijn in de aangezochte staat, of bij iemands vervolging voor abortus als deze persoon woonachtig is in een staat waar abortus wettelijk is toegestaan. Het beginsel van de dubbele strafbaarheid gaat ook vaak vergezeld van aanvullende beperkingen of waarborgen ten aanzien van de sancties, als deze in de verzoekende staat en de tenuitvoerleggingsstaat te sterk uiteenlopen. Het belangrijkste voorbeeld hiervan is de verplichting in bepaalde rechtshulpverdragen om de doodstraf niet toe te passen indien deze straf in de wetgeving van een van beide partijen niet voorkomt.

Volgens de EDPB wordt het beginsel van de dubbele strafbaarheid in het voorstel voor een verordening inzake elektronisch bewijsmateriaal uitgesloten. Dit resulteert echter niet alleen in de tenietdoening van de gebruikelijke formaliteiten van wederzijdse erkenning, maar ook van de waarborgen die samenhangen met het beginsel van de dubbele strafbaarheid zelf.

Volgen de EDPB wordt er namelijk niet verwezen naar de wetgeving van het land waar de aangezochte dienstverlener is gevestigd en is de bewaring van willekeurige gegevens, alsmede de verstrekking van abonnee- en toegangsgegevens, mogelijk voor alle strafbare feiten[10], ongeacht of andere lidstaten vergelijkbare strafbare feiten kennen.

Ondertussen mogen verstrekkingsbevelen alleen worden uitgevaardigd en uitgevoerd wanneer voor hetzelfde strafbare feit in een vergelijkbare binnenlandse situatie in de uitvaardigende staat een soortgelijke maatregel beschikbaar is[11]. Voorts wordt, zoals de Commissie in haar toelichting bij het voorstel voor een verordening schetst, de specificiteit van transactiegegevens en inhoudelijke gegevens bepaald, omdat deze als gevoeliger worden aangemerkt. Bevelen die betrekking hebben op transactiegegevens of inhoudelijke gegevens zijn namelijk gebaseerd op een drempel van een maximale vrijheidsstraf van ten minste drie jaar om ervoor te zorgen dat het evenredigheidsbeginsel en de rechten van de betrokken personen worden geëerbiedigd[12]. De EDPB benadrukt echter dat binnen de EU nog geen harmonisatie heeft plaatsgevonden van strafbare feiten waarvoor een maximale vrijheidsstraf staat van ten minste drie jaar.

De EDPB verzet zich tegen de afschaffing van het beginsel van de dubbele strafbaarheid, dat ervoor moet zorgen dat een staat geen hulp van buitenaf kan krijgen door zijn nationale strafrecht buiten zijn

[9] Artikel 5, lid 1, onder a), AVG.
[10] Artikel 5, lid 3, en artikel 6, lid 2, van het voorstel voor een verordening inzake elektronisch bewijsmateriaal.
[11] Artikel 5, lid 2, van het voorstel voor een verordening inzake elektronisch bewijsmateriaal.
[12] Artikel 5, lid 4, onder a), van het voorstel voor een verordening inzake elektronisch bewijsmateriaal.

landsgrenzen te laten toepassen via een staat die een ander strafrecht hanteert. Dit geldt met name vanwege het verdwijnen van andere belangrijke, traditionele, strafrechtelijke waarborgen (zie punt 3 over locatiecriteria en punt 7, onder g, over potentiële conflicten met het recht van een derde land).

c) Gevolg van de directe benadering van bedrijven

De EDPB erkent dat elektronisch bewijs in toenemende mate beschikbaar is via private infrastructuur en zich buiten het onderzoekende land, in het bezit van dienstverleners, kan bevinden.

Volgens de EDPB is er op grond van uitspraken van Belgische rechters in zaken tegen *Yahoo*[13]! en *Skype*[14], en gelet op terroristische dreigingen, een soepelere en snellere samenwerking tussen publieke en private entiteiten nodig. In haar effectbeoordeling verwijst de Commissie naar drie verschillende procedurele instrumenten, waarbij zowel overheidsinstanties als dienstverleners betrokken zijn. Dit zijn justitiële samenwerking, directe samenwerking en directe toegang. Terwijl bij het eerste instrument de verantwoordelijkheid voor de uitvoering van het EOB niet bij de dienstverlener wordt gelegd, maar bij de uitvoerende staat[15], gaat het tweede, de directe samenwerking, uit van de medewerking van de dienstverlener. Vanuit het oogpunt van een dienstverlener is de directe toegang het meest indringende instrument, omdat overheidsinstanties in dat geval zonder tussenkomst van een intermediair toegang tot gegevens kunnen krijgen.

Daarom vreest de EDPB dat wanneer dienstverleners rechtstreeks worden benaderd, zij persoonsgegevens minder goed kunnen beschermen dan overheidsinstanties dat kunnen en verplicht zijn te doen. Het benadrukt bovendien dat dit tot gevolg kan hebben dat bepaalde procedurele waarborgen waarin ten aanzien van de justitiële samenwerking wordt voorzien voor individuen en bedrijven, niet kunnen worden toegepast[16]. Zo zou een aangezochte dienstverlener naar de rechter in een andere (lid-)staat moeten stappen om tegen het bevel beroep aan te tekenen, terwijl die zich bij justitiële samenwerking tot de autoriteiten in de eigen staat zou moeten richten. De EDPB adviseert aanvullende gronden in het voorstel voor een verordening op te nemen, die moeten waarborgen dat dienstverleners grondrechten van het individu, zoals de bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven en het familie- en gezinsleven, maar ook de informatie van de bevoegde gegevensbeschermingsautoriteit, beschermen om controle mogelijk te maken.

3. Nieuwe grond voor jurisdictie en zogenoemde verdwijning van de locatiecriteria

Volgens de EDPB onderstreept de Commissie dat een van de belangrijkste veranderingen die deze voorstellen met zich meebrengen, ligt in de verdwijning van de locatiecriteria en de mogelijkheid voor

[13] Hof van Cassatie van België, YAHOO! Inc., Nr. P.13.2082.N van 1.12.2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen van België, Nr. ME20.F1.105151-12 van 27.10.2016 (Skype is tegen deze beslissing in beroep gegaan).
[15] Artikelen 10 – 16.
[16] Zie ook vanuit het oogpunt van internationale gegevensbescherming het "Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes" (werkdocument inzake normen voor de bescherming van gegevens en de persoonlijke levenssfeer bij grensoverschrijdende gegevensverzoeken voor handhavingsdoeleinden op het gebied van strafrecht), van de internationale werkgroep inzake gegevensbescherming bij telecommunicatie, 63e vergadering, 9-10.4.2018, Boedapest (Hongarije).

de bevoegde autoriteiten te verzoeken om de bewaring of verstrekking van gegevens, ongeacht waar deze gegevens zijn opgeslagen.

Vanuit gegevensbeschermingsperspectief is het niet nieuw dat EU-wetgeving inzake gegevensbescherming van toepassing is, ongeacht waar persoonsgegevens zijn opgeslagen. De toepasselijkheid van de AVG hangt namelijk af van het feit of de verwerkingsverantwoordelijke of verwerker binnen de EU gevestigd is of dat de gegevens van betrokkenen uit de EU verwerkt worden, ook als de verwerkingsverantwoordelijke of verwerker niet gevestigd is binnen de EU[17], in welk geval zij een wettelijke vertegenwoordiger binnen de EU zullen moeten aanwijzen[18]. Vanuit gegevensbeschermingsperspectief moet worden opgemerkt dat de uitgebreide territoriale werkingssfeer gericht is op een meer volledige bescherming van betrokkenen uit de EU, ongeacht waar het bedrijf dat hun gegevens verwerkt, is gevestigd.

Ondanks dat de verdwijning van de locatiecriteria nieuw is voor het strafrecht, lijkt dit vanuit gegevensbeschermingsperspectief dan ook geen grote verandering te zijn. Volgens de EDPB is er bovendien nog steeds een verband met EU-grondgebied, omdat uitsluitend dienstverleners die diensten aanbieden binnen de Unie onder de werkingssfeer van de voorstellen vallen. Daarnaast impliceert het feit dat uitsluitend in het kader van strafrechtelijke onderzoeken verzoeken gedaan kunnen worden, dat er een verband bestaat met de EU (ofwel omdat een strafbaar feit gepleegd is op het grondgebied van een lidstaat, of omdat het slachtoffer of de pleger van het strafbare feit onderdaan is van een lidstaat).

Indien de locatiecriteria nu uit het strafrecht zouden verdwijnen, zou de EDPB zich vooral zorgen maken over hoe gewaarborgd kan worden dat deze ontwikkeling niet schadelijk is voor de gegevensbescherming en het strafprocesrecht ten aanzien van de betrokkenen en de aangezochte dienstverleners. Wat dat betreft erkent de EDPB dat procedurele waarborgen binnen de EU, in ieder geval ten dele, zijn geharmoniseerd en in acht moeten worden genomen op grond van het Europees verdrag voor de rechten van de mens. Daarom kan gesteld worden dat, onder de voorwaarden die zijn vastgelegd in de ontwerpverordening inzake elektronisch bewijsmateriaal, de gevolgen van de verdwijning van de locatiecriteria waarschijnlijk minder ernstig zullen zijn wanneer bewijs vergaard wordt binnen de EU, dan wanneer autoriteiten uit derde landen gegevens aanvragen bij bedrijven binnen de EU. De EDPB maakt zich dan ook met name zorgen of dit niet tot meer problematische situaties zal leiden. In dit verband zouden autoriteiten uit een derde land waar binnen het strafrecht andere en mogelijk minder procedurele waarborgen bestaan, toegang krijgen tot gegevens die binnen de EU door aanvullende waarborgen worden beschermd. Wat dat betreft wijst de EDPB er nogmaals op dat het zich zorgen maakt over een dubbele standaard en een verzwakking van de fundamentele rechten als dienstverleners en betrokkenen niet kunnen profiteren van procedurele waarborgen uit het EU-recht op het moment dat een aanvraag afkomstig is van een autoriteit uit een derde land.

Aangezien deze nieuwe grond voor jurisdictie "ongeacht de locatie van de gegevens" gekoppeld is aan een procedure die hoofdzakelijk berust op directe verzoeken van bevoegde autoriteiten aan dienstverleners, maakt de EDPB zich bovendien zorgen dat waarborgen voor de bescherming van gegevens mogelijk niet worden toegepast door aangezochte particuliere ondernemingen die niet gebonden zijn aan een rechtsinstrument zoals een rechtshulpverdrag, dat traditioneel de uitwisseling van gegevens tussen justitiële autoriteiten regelt en waarborgen biedt. Binnen het kader van rechtshulpverdragen houden met name minimale beschermingswaarborgen bijvoorbeeld

[17] Zie artikel 3, in het bijzonder lid 2.
[18] Zie artikel 27.

vertrouwelijkheidsverplichtingen in en kunnen gegevens op grond van het specificiteitsbeginsel niet voor andere doeleinden worden verwerkt.

Om die reden benadrukt de EDPB nogmaals dat, ook ten aanzien van de doorgifte van gegevens, minimaal de waarborgen uit Richtlijn (EU) 2016/680 zouden moeten worden toegepast en in het bijzonder artikel 39, voor dienstverleners die gevestigd zijn in een derde land waar op dat vlak geen adequaatheidsbesluit bestaat. De EDPB benadrukt in het bijzonder dat deze bepaling met name betrekking heeft op de informatie van de bevoegde gegevensbeschermingsautoriteit in de lidstaat van de bevel(en) uitvaardigende autoriteit en de documentatie van de doorgifte, ook wat betreft de rechtvaardiging van de ondoelmatigheid of de ongepastheid van een doorgifte aan de bevoegde autoriteit van het derde land.

4. Het begrip "dienstverleners" zou beperkt moeten worden of worden uitgebreid met aanvullende waarborgen voor de rechten van betrokkenen

Wat dienstverleners betreft, juicht de EDPB de uitgebreide definitie toe die zowel communicatiediensten als Over-The-Top-diensten (OTT) omvat. Al deze diensten zijn namelijk functioneel gelijk aan elkaar, waardoor de beoogde maatregelen een vergelijkbaar gevolg kunnen hebben voor het recht op privacy en het recht op vertrouwelijkheid van berichten, zoals wordt benadrukt in de verklaring van de Groep artikel 29 en eerder in advies 01/2017 betreffende het voorstel voor de e-privacy-richtlijn. Het voorstel voor een verordening inzake elektronisch bewijsmateriaal richt zich namelijk op dienstverleners die elektronische-communicatiediensten, zoals gedefinieerd in artikel 2, lid 4, van de richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie, diensten van de informatiemaatschappij, zoals gedefinieerd in artikel 1, lid 1, onder b) van Richtlijn (EU) 2015/1535, "voor wie de opslag van gegevens een wezenlijk onderdeel is van de aan de gebruiker verleende dienst, met inbegrip van sociale netwerken, online marktplaatsen die de transacties tussen hun gebruikers mogelijk maken en andere aanbieders van hostingdiensten", of diensten in verband met internetdomeinnamen en IP-nummering, "zoals aanbieders van IP-adressen, domeinnaamregistrators en -registers en aanverwante privacy- en proxydiensten", leveren[19].

Aangezien een dienstverlener in zin van de ontwerpverordening "een natuurlijke of rechtspersoon is die een of meer van de volgende categorieën diensten aanbiedt", maakt de EDPB zich echter zorgen dat dit instrument betrekking kan hebben op zowel verwerkingsverantwoordelijken als verwerkers in de zin van de AVG. Aangezien onder het "aanbieden van diensten", zoals gedefinieerd is in artikel 2, lid 4, van de ontwerpverordening, verstaan wordt dat natuurlijke of rechtspersonen in een of meer lidstaten in staat worden gesteld om gebruik te maken van de vermelde diensten en dat er een reële link is met de bedoelde lidsta(a)t(en), vallen onder deze activiteiten namelijk activiteiten die door een verwerker worden uitgevoerd voor een verwerkingsverantwoordelijke, zoals de opslag van gegevens.

Bijgevolg vreest de EDPB dat zonder beperkingen op te leggen aan dienstverleners die in de zin van de AVG actief zijn als verwerkingsverantwoordelijken en zonder een specifieke verplichting van de verwerker om de verwerkingsverantwoordelijke te informeren als aan diens adres een verstrekkings- of bewaringsbevel wordt uitgevaardigd, de rechten van betrokkenen zouden kunnen worden

[19] Artikel 2, lid 3, onder c), van het voorstel voor een verordening inzake elektronisch bewijsmateriaal.

ontweken. Dit is met name het geval omdat in het kader van mogelijk tegenstrijdige verplichtingen die moeten voorkomen dat de adressaat ontvangen bevelen gebruikt, de justitiële autoriteiten in de ontwerpverordening ook worden aangemoedigd zich te richten tot de meest geschikte actor, ongeacht de toepasselijke gegevensbeschermingsregels, vooral omdat om allerlei gegevens kan worden verzocht en niet alleen om persoonsgegevens die onder de AVG vallen[20].

Op grond van de AVG handelt een verwerker slechts naar de instructies van de verwerkingsverantwoordelijke. Het is dan ook de verantwoordelijkheid van de verwerkingsverantwoordelijke om de rechten van betrokkenen te waarborgen en hun te voorzien van relevante informatie, onder andere ten aanzien van de adressaten van hun gegevens, bijvoorbeeld in verband met de uitoefening van hun recht van toegang. De verwerker zal dergelijke verzoeken niet van betrokkenen ontvangen en zal deze niet kunnen inwilligen, tenzij de verwerkingsverantwoordelijke daar uitdrukkelijk om heeft verzocht.

Bijgevolg benadrukt de EDPB dat betrokkenen die profiteren van de toepassing van de AVG, tenzij hun rechten beperkt zijn onder de AVG, mogelijk niet in staat zullen zijn hun rechten doelmatig uit te oefenen als de verwerkingsverantwoordelijke niet in de positie verkeert volledige informatie te verstrekken. Volgens de EDPB zal het bovendien nog waarschijnlijker zijn dat geen informatie voorhanden is indien er geen specifieke verplichting op de verwerker rust om de verwerkingsverantwoordelijke te informeren als gegevens waarom verzocht is, betrekking hebben op betrokkenen die niet profiteren van de door de AVG geboden bescherming. De justitiële autoriteiten die om de gegevens verzoeken, zullen in dat geval namelijk niet noodzakelijkerwijs verplicht zijn betrokkenen te informeren over wat zij zelf verder met de gegevens zullen doen. Daarom verzoekt de EDPB om de inperking van de reikwijdte voor verwerkingsverantwoordelijken in de zin van de AVG of om een bepaling op te nemen waaruit blijkt dat in het geval dat de aangezochte dienstverlener niet de verwerkingsverantwoordelijke van de gegevens is, die de verwerkingsverantwoordelijke moet informeren.

5. Er moet duidelijk onderscheid worden gemaakt tussen de begrippen "vestiging" en "wettelijk vertegenwoordiger" in het kader van deze voorstellen en dezelfde begrippen in het kader van de AVG

Aangezien de locatiecriteria niet van toepassing zijn op gegevens, kunnen adressaten van verstrekkings- en bewaringsbevelen binnen de werkingssfeer van het voorstel voor een verordening uitsluitend dienstverleners zijn die diensten verlenen binnen de Unie. Het maakt daarbij niet uit of zij binnen of buiten de EU gevestigd zijn, maar zij zijn op grond van de ontwerprichtlijn wel verplicht een wettelijk vertegenwoordiger aan te wijzen. De begrippen "vestiging" en "wettelijk vertegenwoordiger" worden daarom gedefinieerd in de ontwerpinstrumenten.

Volgens de EDPB komen deze begrippen ook voor in de context van andere EU-instrumenten, met name de AVG. Bijgevolg moeten de definities en de afbakening van deze begrippen in de context van de ontwerpvoorstellen en van de AVG worden toegelicht.

[20] Zie artikel 7, leden 3 en 4.

a) Vestiging

De EDPB wijst er wederom op dat het begrip "vestiging" in de context van de ontwerpverordening niet verward mag worden met hetzelfde begrip in de context van de AVG. In de ontwerpverordening wordt in artikel 2, lid 5, namelijk een ruimere definitie gehanteerd dan in de AVG, aangezien gesproken wordt over "de daadwerkelijke uitoefening van een economische activiteit voor onbepaalde tijd door middel van een duurzame infrastructuur van waaruit diensten worden verleend, of een duurzame infrastructuur van waaruit de activiteiten worden beheerd", ongeacht of de verwerking van persoonsgegevens in het kader van de activiteiten van deze vestiging plaatsvindt. Indien "vestiging" in de zin van de AVG ontegensprekelijk zou moeten worden overgenomen in de in de ontwerpverordening opgenomen definitie van vestiging, zou bijgevolg het tegenovergestelde niet het geval kunnen zijn.

Daarom waarschuwt de EDPB dat bij vestigingen van dienstverleners in de zin van de ontwerpverordening niet noodzakelijkerwijs voldaan is aan de voorwaarden voor de toepassing van de AVG volgens artikel 3, lid 1. Verwerkingsverantwoordelijken en verwerkers worden dienaangaande verzocht na te gaan of de toepasselijkheid van de AVG niet gebaseerd is op artikel 3, lid 2, waardoor binnen de EU een wettelijk vertegenwoordiger zou moeten worden aangewezen en geen één-loket-mechanisme aanwezig zou zijn.

b) Wettelijke vertegenwoordiger

De Groep artikel 29 benadrukte in haar verklaring dat verwarring voorkomen moet worden tussen de verplichting om een wettelijk vertegenwoordiger aan te wijzen overeenkomstig artikel 27 van de AVG en de wettelijk vertegenwoordiger waarin de ontwerpverordening inzake elektronisch bewijsmateriaal voorziet.

De EDPB wil aan de hand van het ontwerpvoorstel deze aanbevelingen opnieuw onder de aandacht brengen en met name onderstrepen dat naar zijn mening de wettelijk vertegenwoordiger in de betekenis van de ontwerprichtlijn over de aanwijzing van een wettelijke vertegenwoordiger binnen het kader van de voorstellen betreffende elektronisch bewijs, altijd moet worden aangewezen, dat hieraan specifieke taken moeten worden toegekend, ongeacht een door de dienstverlener verleende volmacht, dat die in staat moet zijn verzoeken in te willigen en op te treden namens de dienstverlener en dat die een grotere verantwoordelijkheid draagt dan de wettelijke vertegenwoordiger volgens de AVG.

Bovendien benadrukt de EDPB dat de verplichting volgens de ontwerpvoorstellen inzake elektronisch bewijsmateriaal om altijd een wettelijk vertegenwoordiger aan te wijzen, ongeacht of de dienstverlener binnen of buiten de EU is gevestigd, de mogelijkheid om voor dezelfde dienstverlener volgens de ontwerprichtlijn voor elektronisch bewijs verschillende wettelijke vertegenwoordigers aan te wijzen en de verplichting om de aanwijzing van de wettelijke vertegenwoordiger bij de autoriteiten van de lidstaten te melden, afwijken van hetgeen de AVG voorschrijft. De AVG voorziet niet in de verplichting de aangewezen wettelijk vertegenwoordiger te melden, in uitzonderingen op de aanwijzing en in beperkte verantwoordelijkheden voor de wettelijke vertegenwoordiger.

Gelet op de aanzienlijke verschillen qua functie, verantwoordelijkheid en betrekking met de andere vestigingen van de dienstverlener in het ene geval en de verwerkingsverantwoordelijke of verwerker in het andere geval, adviseert de EDPB daarom dat indien een dienstverlener niet gevestigd is binnen de EU, maar zowel onder de AVG, op grond van artikel 3, lid 2, als de verordening inzake elektronisch bewijsmateriaal valt, twee verschillende wettelijke vertegenwoordigers aan te wijzen, ieder met

duidelijk afgebakende functies al naar gelang het instrument op basis waarvan de aanwijzing heeft plaatsgevonden.

6. Nieuwe gegevenscategorieën

Het voorstel voor een verordening beschrijft verschillende gegevenscategorieën op grond van artikel 2: abonneegegevens, toegangsgegevens, transactiegegevens en inhoudelijke gegevens. Verder wordt in overweging 20 van het voorstel van de Commissie bepaald: *"De categorieën van gegevens die onder deze verordening vallen, omvatten abonneegegevens, toegangsgegevens, transactiegegevens (de drie categorieën die worden aangeduid als niet-inhoudelijke gegevens) en inhoudelijke gegevens. Dit onderscheid wordt, zij het niet wat betreft toegangsgegevens, in de wetgeving van veel lidstaten gemaakt, alsook in het rechtskader van de VS, dat dienstverleners toestaat op vrijwillige basis niet-inhoudelijke gegevens te delen met buitenlandse rechtshandhavingsinstanties."*

In dit verband benadrukt de EDPB in de eerste plaats dat alle voornoemde vier categorieën van gegevens beschouwd worden als persoonsgegevens op grond van EU-wetgeving inzake gegevensbescherming, omdat zij informatie bevatten over een geïdentificeerde of identificeerbare natuurlijke persoon, ongeacht of in het voorstel voor een verordening naar de betrokkene verwezen wordt als "abonnee" of "gebruiker". Ook moet worden opgemerkt dat onder "elektronisch bewijs" zoals dat wordt gedefinieerd in artikel 2, lid 6, van het Commissievoorstel, alle vier categorieën van gegevens vallen en er daarom een verband bestaat met persoonsgegevens. In plaats van regels vast te leggen voor de toegang tot bewijs, die in nationale wetgeving en justitiële procedures worden gedefinieerd en gekwalificeerd, voorziet het voorstel voor een verordening in nieuwe materiële en procedurele voorwaarden voor de toegang tot persoonsgegevens.

Terwijl in het voorstel voor een verordening nieuwe subcategorieën van persoonsgegevens worden vastgelegd waarop verschillende procedurele voorwaarden voor toegang van toepassing zijn, herinnert de EDPB eraan dat het, overeenkomstig relevante rechtspraak van het HvJ-EU, voor de vaststelling of sprake is van een inbreuk op het grondrecht op privacy, niet uitmaakt of de informatie over de betrokken privélevens een gevoelig karakter heeft of dat de betrokkenen op welke wijze dan ook hinder hebben ondervonden.

Voorts wijst de EDPB erop dat met betrekking tot "niet-inhoudelijke gegevens", waartoe volgens het voorstel van de Commissie abonneegegevens, toegangsgegevens en transactiegegevens behoren, het Hof van Justitie in zijn arrest in de gevoegde zaken C-203/15 en C-698/15 Tele*2 Sverige AB* heeft bepaald dat aan de hand van metadata, zoals verkeersgegevens en locatiegegevens, het profiel van de betrokken personen kan worden bepaald, informatie die, wat het recht op bescherming van het privéleven betreft, even gevoelig is als de inhoud zelf van de communicaties[21].

Zoals ook gesteld is in de verklaring van de Groep artikel 29 van 29 november 2017 over gegevensbescherming en privacyaspecten van grensoverschrijdende toegang tot elektronisch bewijsmateriaal, herhaalt de EDPB zijn twijfels en bezorgdheid ten aanzien van de huidige afbakening van "niet-inhoudelijke" en inhoudelijke gegevens, en van de vier categorieën van persoonsgegevens uit het voorstel voor een verordening. De vier beoogde categorieën lijken namelijk niet duidelijk te zijn afgebakend en de definitie van "toegangsgegevens" is vergeleken met de andere categorieën nog altijd vaag. De EDPB betreurt dan ook dat in de effectbeoordeling en het Commissievoorstel de

[21] Arrest van het HvJ-EU van 21.12.2016, punt 99.

redenen voor het aanmaken van deze nieuwe subcategorieën van persoonsgegevens, niet verder worden onderbouwd en uit zijn bezorgdheid ten aanzien van het andere waarborgniveau voor de materiële en procedurele voorwaarden voor de toegang tot de categorieën van persoonsgegevens, met name gelet op de moeilijkheid om in sommige gevallen praktisch te beoordelen tot welke categorie van gegevens de aangevraagde gegevens behoren. Zo zouden IP-adressen beschouwd kunnen worden als transactiegegevens en abonneegegevens.

In dit verband haalt dde EDPB aan dat in overweging 14 van zijn voorstel voor een verordening betreffende de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens in elektronische communicatie (e-privacy), de Commissie van mening is dat "elektronische-communicatiegegevens [...] voldoende ruim en op technologisch neutrale wijze [moeten] worden gedefinieerd zodat de definitie slaat op alle informatie die betrekking heeft op de doorgegeven of uitgewisselde inhoud (inhoud van elektronische communicatie), alsook op de informatie over eindgebruikers van elektronische-communicatiediensten die verwerkt wordt met het oog op de transmissie, de distributie of de uitwisseling van elektronische-communicatie-inhoud, waaronder gegevens om de bron en de bestemming, de geografische locatie en de datum, het tijdstip, de duur en het soort communicatie te traceren en te omschrijven". Aangezien het huidige en toekomstige e-privacy-kader, alsook de beperkingen van het recht op privacy die dat met zich meebrengt, van toepassing zal zijn op de regels voor de toegang tot elektronisch bewijs in verband met rechtshandhaving, adviseert de EDPB een bredere definitie van elektronische-communicatiegegevens in het voorstel voor een verordening op te nemen om ervoor te zorgen dat de passende waarborgen en voorwaarden voor toegang die moeten worden vastgesteld, ook ruimschoots voor "niet-inhoudelijke" en "inhoudelijke gegevens" gelden.

7. Analyse van de procedures voor Europese verstrekkings- en bewaringsbevelen

De procedure voor het uitvaardigen van een verstrekkings- of bewaringsbevel lijkt in grote lijnen als volgt te verlopen:

- De bevoegde justitiële autoriteit – de uitvaardigende autoriteit – vaardigt, afhankelijk van het soort gegevens waarom wordt verzocht en het soort bevel, het bevel uit met inachtneming van de (weinige) voorwaarden die beschreven worden in de artikelen 5 en 6 en verstuurt deze met gebruikmaking van een geharmoniseerd certificaat naar de wettelijk vertegenwoordiger van de dienstverlener of naar een van diens vestigingen binnen de EU – de adressaat.
- Na ontvangst van het certificaat zal de adressaat het bevel uitvoeren – wat inhoudt dat de gegevens binnen tien dagen of zes uur, in noodgevallen, moeten worden overgedragen of maximaal zestig dagen moeten worden bewaard – tenzij dit onuitvoerbaar is, omdat het certificaat onvolledig is, er sprake is van overmacht of het feitelijk onmogelijk is voor de adressaat of omdat de adressaat weigert op grond van tegenstrijdige verplichtingen, hetzij ten aanzien van grondrechten of fundamentele belangen van een derde land, hetzij vanwege andere gronden.
- Indien de adressaat het uitgevaardigde bevel niet naleeft zonder redenen op te geven die door de uitvaardigende autoriteit worden aanvaard, kunnen procedures worden gestart waarmee de bevelen ten uitvoer kunnen worden gelegd door een bevoegde autoriteit in de lidstaat waar de dienstverlener is vertegenwoordigd of gevestigd, tenzij sprake is van beperkte

weigeringsgronden en de tenuitvoerleggingsautoriteit bezwaar maakt tegen de erkenning of de tenuitvoerlegging van het bevel.

- In het geval dat de adressaat een gemotiveerd bezwaar tegen het bevel heeft ingediend, dat gebaseerd is op tegenstrijdige verplichtingen, zal de uitvaardigende autoriteit de zaak naar de bevoegde rechtbank in de betreffende lidstaat verwijzen, die zich over de vermeende tegenstrijdigheid moet buigen en het bevel moet handhaven indien van tegenstrijdigheid geen sprake is. Indien sprake is van tegenstrijdigheid kan de bevoegde rechtbank zich via haar nationale centrale autoriteiten tot de centrale autoriteiten van het derde land richten. De termijn om te reageren bedraagt vijftien dagen en kan op gemotiveerd verzoek met dertig dagen worden verlengd in geval van tegenstrijdige verplichtingen ten aanzien van grondrechten of fundamentele belangen van een derde land. Maar de bevoegde rechtbank kan zelf ook bepalen of het bevel in stand wordt gehouden of wordt ingetrokken wegens andere door de adressaat aangevoerde weigeringsgronden.
- Onverminderd middelen uit hoofde van de AVG en Richtlijn (EU) 2016/680, hebben personen wier gegevens werden verkregen via een verstrekkingsbevel, recht op doeltreffende rechtsmiddelen tegen dit bevel.

De EDPB heeft de procedures en waarborgen als bedoeld in de ontwerpverordening voor de verschillende stappen beoordeeld en adviseert voor de hierna besproken aspecten de volgende waarborgen en wijzigingen door te voeren.

a) Voor de uitvaardiging van bevelen moeten drempels worden opgeworpen en bevelen moeten worden uitgevaardigd of goedgekeurd door rechtbanken

Wat de voorwaarden voor de uitvaardiging van bevelen betreft, juicht de EDPB uitgebreidere waarborgen voor de toegang tot transactiegegevens of inhoudelijke gegevens toe. Hij merkt echter op dat, gelet op het ontbreken van een volledige harmonisatie van strafrechtelijke sancties tussen lidstaten, met de verwijzing naar "strafbare feiten waarop in de uitvaardigende staat een vrijheidsstraf staat met een maximum van ten minste drie jaar"[22], nog altijd sprake kan zijn van verschillende drempels en afwijkingen in de gegevensbescherming voor betrokkenen binnen de EU.

Bovendien benadrukt de EDPB dat, met name gelet op de ruime omschrijving van abonneegegevens, de beoogde drempel nogal laag lijkt te zijn voor verstrekkings- en bewaringsbevelen betreffende abonneegegevens of toegangsgegevens, aangezien alle strafbare feiten in beginsel de uitvaardiging van deze bevelen rechtvaardigen. Ook kennen de autoriteiten die zulke bevelen mogen uitvaardigen, meer beperkingen als het gaat om verstrekkingsbevelen betreffende transactiegegevens of inhoudelijke gegevens dan bij de uitvaardiging van bewarings- of verstrekkingsbevelen betreffende abonneegegevens of toegangsgegevens. Openbare aanklagers mogen namelijk alleen de laatstgenoemde bevelen uitvaardigen, terwijl een rechter, rechtbank of onderzoeksrechter elk bevel mag uitvaardigen of goedkeuren.

De EDPB betreurt in het bijzonder dat de laagste drempel die het voor rechtshandhavingsinstanties mogelijk maakt voor alle strafbare feiten om toegang tot abonneegegevens en toegangsgegevens te

[22] Zie artikel 5, lid 3, onder a).

verzoeken, steunt op een *"a contrario"* uitleg van de rechtspraak van het HvJ-EU (die gericht is op de andere gegevens) om onderscheid aan te brengen in de mogelijke waarborgen. Het HvJ-EU heeft namelijk specifiek benadrukt dat voor wat betreft verkeersgegevens en locatiegegevens de bevoegde autoriteiten alleen toegang wordt verleend voor de bestrijding van ernstige criminaliteit[23]. De EDPB zou er begrip voor kunnen hebben dat het voorstel zou voorzien in de mogelijkheid om zonder voorafgaande goedkeuring van een rechtbank toegang te verkrijgen tot zeer basale informatie die net voldoende is om iemand te identificeren zonder communicatiegegevens openbaar te maken. Het betreurt echter de ruime *"a contrario"* uitleg van dit oordeel door de Commissie en roept op tot de invoering van uitgebreidere waarborgen om de gronden voor toegang tot andere abonneegegevens en toegangsgegevens te beperken. DDe EDPB stelt voor de toegang tot deze gegevens te beperken tot een in de ontwerpverordening opgenomen lijst van strafbare feiten of ten minste tot "ernstige strafbare feiten", met name gelet op de lagere drempel voor voorafgaande goedkeuring waarin voor deze gegevens is voorzien.

Daarnaast onderstreept de EDPB dat deze *"a contrario"* uitleg er ook toe leidt dat het voorstel openbaar aanklagers de mogelijkheid biedt bevelen uit te vaardigen of de uitvaardiging van bevelen goed te keuren. De EDPB is van mening dat, behalve wanneer sprake is van verzoeken om zeer basale informatie die net voldoende is om iemand te identificeren zonder communicatiegegevens openbaar te maken, in dit geval een stap terug wordt gezet ten opzichte van de rechtspraak van het HvJ-EU betreffende de toegang tot communicatiegegevens. In zijn rechtspraak betreffende toegang tot communicatiegegevens ten behoeve van rechtshandhaving, heeft het HvJ-EU inderdaad, naast andere criteria, grenzen gesteld aan de mogelijkheid om in deze toegang te voorzien, en is die *"behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid"*[24], *"onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit"*, *"op een met redenen omkleed verzoek van deze autoriteiten dat met name is ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten."*[25]

De EDPB herhaalt dat het begrip "rechtbank" een volledig autonoom begrip van Unierecht is en dat het HvJ-EU voortdurend de criteria waaraan voldaan moet worden om als rechtbank te kunnen worden aangemerkt, heeft benadrukt en opnieuw heeft aangevoerd. Daartoe behoren ook de criteria voor onafhankelijkheid[26], waarvan geen sprake lijkt te zijn bij openbaar aanklagers, zoals ook blijkt uit jurisprudentie van het EHRM[27].

Bijgevolg resulteren de artikelen 4, lid 1, onder a) en b), en 3, onder a) en b), in procedures die aanzienlijk minder waarborgen bieden voor abonneegegevens en toegangsgegevens. Een openbaar aanklager kan immers zelf om gegevens verzoeken, zonder verder toezicht door de autoriteit van de staat waar de aangevraagde gegevens zich bevinden of door de autoriteit waar zich de wettelijk vertegenwoordiger of het aangezochte bedrijf bevindt, of zonder toezicht van een onafhankelijke bestuurlijke autoriteit.

Bovendien haalt de EDPB de zogeheten aanvullende waarborg uit artikel 5, lid 2, aan, die de mogelijkheid om een verstrekkingsbevel uit te vaardigen beperkt wanneer voor hetzelfde strafbare feit in een vergelijkbare binnenlandse situatie een vergelijkbare maatregel beschikbaar is. Hij waarschuwt echter dat deze maatregelen contraproductief kunnen werken: in plaats van aanvullende

[23] Zie zaak 203/15, punt (125).
[24] Zie zaak 203/15, punt (120).
[25] Zie de gevoegde zaken C-293/12 en C-594/12, punt (62).
[26] Zie bijvoorbeeld zaak C-203/14.
[27] Zie bijvoorbeeld Moulin c/ France 23/11/2010.

waarborgen te bieden, lijkt het de lidstaten eerder aan te sporen tot uitbreiding van hun nationale mogelijkheden voor het indienen van verzoeken om verstrekking van abonnee- of toegangsgegevens met als doel ervoor te zorgen dat verstrekkingsbevelen uit hoofde van deze verordening kunnen worden uitgevaardigd.

b) Termijnen voor het verstrekken van gegevens moeten worden verantwoord

Volgens de EDPB moeten Europese verstrekkingsbevelen, zoals bepaald in artikel 9, leden 1 en 2, binnen uiterlijk tien dagen na ontvangst van het certificaat worden beantwoord, tenzij de uitvaardigende autoriteit redenen aanvoert voor eerdere openbaarmaking, en in noodgevallen binnen uiterlijk zes uur.

Volgens de EDPB ontbreekt het echter aan criteria op basis waarvan de verplichting voor autoriteiten om de noodzaak van gegevensverstrekking aan te tonen, ook achteraf om enig toezicht op het gebruik van deze zeer snelle procedure mogelijk te maken, in een kader is vervat. Dat terwijl een termijn van zes uur waarschijnlijk tot gevolg zal hebben dat voorafgaand aan de gegevensverstrekking slechts een zeer summier toezicht zal plaatsvinden, of bij de dienstverlener elke vorm van toezicht ontbreekt. Uit de effectbeoordeling blijkt namelijk dat het voor bevoegde autoriteiten noodzakelijk is dat zij tijdig toegang krijgen tot gegevens. De in de effectbeoordeling gegeven voorbeelden hebben allemaal betrekking op bewijs dat nodig was in ernstige misdrijven (gevallen van terrorisme met gijzeling, voortdurend seksueel misbruik van kinderen), maar de rechtvaardiging op basis van het vluchtige karakter van bewijs, lijkt ontoereikend als geen sprake is van een andere specifieke urgentie dan de eventuele vluchtigheid van gegevens. Bovendien biedt het vluchtige karakter van gegevens geen aanvullende rechtvaardiging wat betreft de evenredigheid voor toegang tot gegevens met minder waarborgen in deze situaties waarin geen andere urgentie bestaat dan de vluchtigheid van gegevens.

Bovendien twijfelt de EDPB over de noodzaak van een termijn van zes uur als deze termijn, zoals voorzien, pas van toepassing zou zijn als de uitvaardigende autoriteit "binnen vijf dagen" aanvullende toelichtingen verschaft in het geval dat de dienstverlener niet aan zijn verplichting kan voldoen.

De EDPB roept daarom op tot aanvullingen in de effectbeoordeling om de noodzaak van deze termijnen in gevallen waarin het gepleegde of vervolgde strafbare feit niet ernstig is, te rechtvaardigen en, tenzij zulke gedetailleerde aanvullingen worden doorgevoerd, tot het opstellen van expliciete criteria die de urgentie voor de uitvaardiging van Europese verstrekkingsbevelen, moeten rechtvaardigen. Het zou bijvoorbeeld mogelijk zijn het model uit de EOB-richtlijn te volgen. De EOB-richtlijn voorziet in een kortere termijn als die gerechtvaardigd wordt door "proceduretermijnen, de ernst van het strafbaar feit of andere bijzonder dringende omstandigheden" (zie artikel 12, lid 2), of in een termijn van 24 uur, waarin een beslissing moet worden genomen over voorlopige maatregelen (zie artikel 32, lid 2). De effectbeoordeling van de ontwerpverordening geeft geen gedetailleerde rechtvaardiging voor de reden waarom deze termijnen niet werken. Het enige wat naar voren komt is dat het aantal gedane verzoeken de ontvangende justitiële autoriteiten overbelasten, waardoor zij de termijnen niet kunnen naleven.

c) Europese verstrekkings- of bewaringsbevelen mogen niet gebruikt worden om gegevens, met name inhoudelijke gegevens, over betrokkenen uit een andere lidstaat aan te vragen, zonder de bevoegde autoriteiten van die lidstaat te informeren

De EDPB herhaalt dat bestaande instrumenten voorzien in justitiële samenwerking en derhalve in aanvullende waarborgen, met name voor het toezicht op de noodzaak en de evenredigheid van verzoeken. Het benadrukt dat deze waarborgen des te meer gerechtvaardigd zijn in gevallen waarin om inhoudelijke gegevens is verzocht, waarvoor grotere beperkingen gelden ten aanzien van de rechten op bescherming van de persoonsgegevens en de privacy van betrokkenen. In dit verband herhaalt de EDPB dat de EOB-richtlijn ook de mogelijkheid biedt van interceptie van telecommunicatie met technische bijstand van een andere lidstaat (zie artikel 30). Daarnaast voorziet de richtlijn in de verplichting van kennisgeving van de interceptie van gegevens aan de bevoegde autoriteit van een andere lidstaat waar de persoon op wie de interceptie betrekking heeft, zich bevindt en van welke geen bijstand vereist is (zie artikel 31).

De EDPB vindt geen rechtvaardiging voor de procedure uit de ontwerpverordening voor elektronisch bewijs om de verstrekking van inhoudelijke gegevens mogelijk te maken, zonder betrokkenheid van ten minste de bevoegde autoriteiten van de lidstaat waar de betrokkene zich bevindt.

d) Europese bewaringsbevelen mogen niet gebruikt worden om verplichtingen tot bewaring van gegevens van de dienstverleners te omzeilen

Volgens de EDPB is het hoofddoel van Europese bewaringsbevelen te voorkomen dat gegevens worden gewist.

Hoewel de EDPB erkent dat het in sommige gevallen noodzakelijk en evenredig kan zijn, betreurt hij het gebrek aan waarborgen voor de uitvaardiging van deze bevelen. De EDPB adviseert met name dat wanneer bewaringsbevelen voor uitsluitend specifieke gegevens worden uitgevaardigd, waarvoor het ontwerp ruime verzoekmogelijkheden lijkt te bieden, en deze bevelen worden uitgevaardigd voor gegevens die overeenkomstig het beginsel van gegevensbewaring gewist moeten worden, het bevel voor de dienstverlener nooit als basis mag dienen om de gegevens na de oorspronkelijke wisdatum te verwerken. Gegevens moeten, met andere woorden, worden "bevroren".

Bovendien moet het verband tussen het bewaringsbevel en het aansluitende verzoek om gegevens te verstrekken, ongeacht of dat gebeurt door middel van een Europees verstrekkingsbevel, een EOB-verzoek of een wederzijds rechtshulpverzoek, versterkt worden om ervoor te zorgen dat Europese bewaringsbevelen alleen worden uitgevaardigd als het andere verzoek zeker is (en niet slechts als mogelijkheid wordt overwogen) en dat wanneer het andere verzoek wordt geweigerd, ook het bewaringsbevel verloopt, zonder dat zestig dagen gewacht hoeft te worden[28] als het aansluitende verzoek eerder is geweigerd.

e) Vertrouwelijkheid en gebruikersinformatie

Volgens de EDPB is een specifiek artikel[29] betreffende de vertrouwelijkheid van bevelen in de ontwerpverordening geïntroduceerd. Om verwarring en onbegrip ten aanzien van het recht op bescherming van persoonsgegevens te voorkomen, herinnert de EDPB eraan dat de AVG er weliswaar in voorziet dat beperkingen van de rechten van betrokkenen om het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten te waarborgen, wettelijk zouden moeten worden vastgelegd en derhalve openbaar zouden moeten zijn[30] en dat deze wettelijke maatregelen specifieke

[28] Zie artikel 10, lid 1.
[29] Zie artikel 11.
[30] Zie artikel 23, lid 1, onder d).

bepalingen moeten bevatten ten aanzien van het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking[31], maar juist niet voorziet in de verplichting om betrokkenen individueel te informeren over ieder toegangsverzoek dat door rechtshandhavingsinstanties wordt ingediend.

De EDPB herinnert er ondertussen aan dat de gegevensbeschermingsrichtlijn in dit kennisgevingsrecht voor de betrokkenen door de bevoegde autoriteiten voorziet, tenzij dit recht beperkt is, voor iedere betrokkene zonder dit recht alleen te beperken voor betrokkenen die woonachtig zijn op het grondgebied van de EU.

f) Procedure voor de tenuitvoerlegging van een bevel bij weigering van de dienstverlener deze uit te voeren

Volgens de EDPB voorziet artikel 14 van de ontwerpverordening in een procedure die de tenuitvoerlegging van een bevel moet waarborgen als de adressaat deze niet naleeft. Deze procedure is gebaseerd op een justitiële samenwerking tussen de uitvaardigende autoriteit en een bevoegde autoriteit in de uitvaardigende staat.

Het lijkt er echter op dat de tenuitvoerleggingsautoriteit volgens deze procedure de uitvoering van het doorgegeven bevel niet mag weigeren op andere dan procedurele gronden (zoals ook voor de adressaat geldt, met name het gebrek aan aangeleverde informatie of de feitelijke onmogelijkheid gegevens te verstrekken), omdat de betrokken gegevens beschermd zijn door een immuniteit of voorrecht krachtens haar eigen nationale recht of omdat de openbaarmaking ervan de fundamentele belangen van die lidstaat zou kunnen schaden, onder meer op het gebied van nationale veiligheid en defensie[32].

Daarom spreekt de EDPB opnieuw zijn bezorgdheid uit over het wegnemen van dubbele controles van het doorgegeven bevel door de ontvangende bevoegde autoriteit, vergeleken met de andere instrumenten. Zelfs de grond voor de weigering een bevel ten uitvoer te leggen op grond van strijdigheid met het Handvest, lijkt een grotere drempel te zijn dan de klassieke drempel betreffende de inbreuk op de grondrechten van de betrokken persoon. In navolging van de voorbeelden van het Europees aanhoudingsbevel, dat voorziet in verplichte en optionele weigeringsgronden, of ten minste de EOB-richtlijn, die er in algemene zin in voorziet dat het vermoeden dat "het scheppen van een ruimte van vrijheid, veiligheid en recht binnen de Unie is gebaseerd op wederzijds vertrouwen en een vermoeden van naleving door de andere lidstaten van het recht van de Unie, en met name van de grondrechten" weerlegbaar is[33], moet de ontwerpverordening bijgevolg ten minste voorzien in de traditionele afwijkende bepaling dat, indien er gegronde redenen zijn om aan te nemen dat de uitvoering van een bevel in een inbreuk op een grondrecht van de betrokkene zou resulteren en dat de tenuitvoerleggingsstaat zijn verplichtingen betreffende de bescherming van de grondrechten die zijn vervat in het Handvest niet zou nakomen, de tenuitvoerlegging van het bevel moet worden geweigerd.

g) Tenuitvoerlegging van bevelen en tegenstrijdige verplichtingen uit hoofde van het recht van een derde land (artikelen 15 en 16)

[31] Zie artikel 23, lid 2, onder h).
[32] Zie artikel 14, lid 2.
[33] Zie overweging 19 van de EOB-richtlijn.

De EDPB juicht de mogelijkheid uit de ontwerpverordening toe dat adressaten een bevel mogen weigeren op de grond dat het strijdig is met grondrechten, aangezien het bedoeld is om waarborgen te bieden in het geval van tegenstrijdige wettelijke verplichtingen. Het acht het ook essentieel dat het voorstel, in ieder geval indien zich een tegenstrijdigheid voordoet, voorziet in de raadpleging van autoriteiten van derde landen en in de verplichting het bevel in te trekken als de autoriteit van een derde land bezwaar maakt.

Daarom moet de beoogde procedure die het mogelijk maakt de uitvoering van een bevel te weigeren op grond van tegenstrijdige verplichtingen uit hoofde van het recht van een derde land, aanzienlijk worden verbeterd.

In de eerste plaats is het volgens de EDPB het geval dat de ontwerpverordening een privaat bedrijf, als adressaat van een verstrekkingsbevel, belast met de beoordeling of een bevel al dan niet strijdig is met het toepasselijke recht van een derde land, waardoor de openbaarmaking van de gevraagde gegevens wordt belet. Het bedrijf moet een gemotiveerd bezwaar aandragen met alle relevante informatie over het recht van het derde land, over de toepasselijkheid ervan op de betrokken zaak en over de aard van de tegenstrijdige verplichtingen.

De EDPB maakt zich het meest zorgen dat wanneer in dat opzicht bezwaar wordt gemaakt, de bevoegde rechtbank van de lidstaat van de uitvaardigende autoriteit alleen beoordeelt of al dan niet sprake is van tegenstrijdigheid, aangezien uitsluitend in het geval dat de rechtbank een tegenstrijdigheid vaststelt, contact moet worden gezocht met de autoriteiten van het derde land. Het is dus aan de bevoegde EU-rechtbank om op dat vlak een sluitende interpretatie van het recht van een derde land te geven, terwijl deze rechtbank op dat gebied nauwelijks over voldoende deskundigheid beschikt. De EDPB is van oordeel dat de verplichting om de bevoegde autoriteiten van het derde land te raadplegen, in het huidige voorstel dan ook tekort schiet. Ten aanzien van de gegevensbescherming wijst de EDPB de wetgever op het feit dat wanneer een bevoegde rechtbank van een derde land op grond van de AVG zou beoordelen of er op basis daarvan sprake is van tegenstrijdigheid met eigen vereisten, de gegevensbeschermingsautoriteiten van de EU en de bevoegde rechtbanken de bevoegdheid zouden blijven houden om de rechtmatigheid van de doorgifte te beoordelen op basis van een rechterlijke uitspraak of van een besluit van een administratieve autoriteit van een derde land op grond waarvan persoonsgegevens moeten worden doorgegeven of verstrekt binnen de reikwijdte van de AVG[34].

Daarnaast onderstreept de EDPB dat de beoordeling van het recht van het derde land door de bevoegde rechtbank van de verzoekende EU-lidstaat gebaseerd moet zijn op objectieve redenen en hij is bezorgd over de criteria waarmee de bevoegde rechtbank rekening moet houden bij de beoordeling van het recht van het derde land overeenkomstig artikel 15, lid 4, en artikel 16, lid 5, onder a), van de ontwerpverordening. De rechtbank zou dan inderdaad moeten kijken naar het feit dat het recht van het derde land "niet zozeer de grondrechten of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging beoogt te beschermen", maar "er kennelijk op is gericht andere belangen te beschermen of illegale activiteiten af te schermen tegen verzoeken van rechtshandhavingsinstanties in het kader van strafrechtelijk onderzoek" of "het belang dat wordt beschermd door het relevante recht van het derde land, met inbegrip van het belang van het derde land bij niet-openbaarmaking van de gegevens". Bijvoorbeeld, hoewel deze beoordeling vanwege, in ieder geval, de potentiële gevolgen van een dergelijke beslissing in principe gebaseerd zou moeten zijn

[34] Zie artikel 48 AVG.

op op grond van alle beschikbare informatie verkregen bewijs, zorgt de formulering ("kennelijk op is gericht") voor onduidelijkheid en zou deze moeten worden aangepast ("is erop gericht/heeft als doel").

De EDPB betreurt het dat het enige geval waarin de autoriteiten van een derde land geraadpleegd zouden worden en bezwaar zouden kunnen maken tegen de uitvoering van een verstrekkingsbevel zich zou voordoen wanneer naar het oordeel van deze bevoegde EU-rechtbank sprake zou zijn van tegenstrijdigheid, zij alle details hiervan zou overdragen aan de centrale autoriteiten van het betrokken derde land en de centrale autoriteit van dat derde land bezwaar zou maken binnen de krappe termijn van maximaal vijftig dagen (vijftien dagen, eventueel verlengd met dertig dagen en vijf extra dagen voor de laatst mogelijke herinnering). In alle andere gevallen zou de bevoegde rechtbank in de positie zijn het verstrekkingsbevel in stand te houden en een geldboete op te leggen aan de dienstverlener die weigert het bevel uit te voeren. Bijgevolg is de EDPB bezorgd dat de bevoegde EU-rechtbanken geen verdere verplichting zouden hebben om de bevoegde autoriteiten van de betrokken derde landen te raadplegen om ervoor te zorgen dat de procedure een systematischer waarborg zou bieden dat de argumenten van beide zijden in aanmerking worden genomen en er meer respect is voor het recht van derde landen.

Zoals in de verklaring van de Groep artikel 29 en hierboven reeds is benadrukt, herinnert de EDPB eraan dat extra aandacht moet worden geschonken aan de vaststelling door derde landen van vergelijkbare instrumenten die mogelijk de rechten van betrokkenen en hun recht op privacy binnen de EU, met name het risico van vergelijkbare instrumenten die direct in strijd zijn met EU-wetgeving inzake gegevensbescherming, kunnen schaden.

Daarnaast onderstreept de EDPB dat de bevoegde rechtbank van de lidstaat van de uitvaardigende autoriteit mogelijk niet de rechtbank zal zijn die bevoegd is om het bevel uit hoofde van artikel 14 van de ontwerpverordening ten uitvoer te leggen, waardoor het risico van tegenstrijdige procedures en het gebrek aan tegencontroles in geval van tegenstrijdig recht, toeneemt. Dit vloeit voort uit het feit dat er in sommige gevallen drie staten bij betrokken kunnen zijn: de staat van de autoriteit die het bevel uitvaardigt, het derde land van de dienstverlener en de lidstaat waar zich de wettelijk vertegenwoordiger van de dienstverlener in de EU bevindt en waar het bevel ten uitvoer zou moeten worden gelegd. Volgens de procedure die momenteel is opgenomen, zou bijgevolg de rechtbank van de verzoekende autoriteit in lidstaat A haar eigen interpretatie aan het recht van het derde land B van de dienstverlener kunnen geven, zonder daarin de zienswijzen van de autoriteiten van dit derde land mee te nemen (terwijl zij tegen het bevel bezwaar zouden hebben gemaakt), en een rechtbank van een andere EU-lidstaat C verzoeken haar beslissing ten uitvoer te leggen zonder de mogelijkheid van bezwaar.

Verder juicht de EDPB ook de invoering toe van specifieke rechtsmiddelen tegen verstrekkingsbevelen, die een aanvulling moeten vormen op de rechtsmiddelen uit de AVG en Richtlijn (EU) 2016/680. De Groep artikel 29 heeft in haar eerdere verklaring al tot zulke rechtsmiddelen opgeroepen. De EDPB betreurt echter dat voor bewaringsbevelen niet in dergelijke rechtsmiddelen is voorzien, aangezien deze bevelen ook tot beperkingen kunnen leiden van de grondrechten van personen van wie gegevens worden bewaard. Bewaringsbevelen kunnen namelijk tot gevolg hebben dat gegevens langer bewaard worden dan op grond van gegevensbeschermingsregels mogelijk zou zijn. Het bewaringsbevel op zich zorgt dus voor een beperking van de grondrechten van de betrokkene en voor de rechtvaardiging ervan gelden een toetsing en specifieke rechtsmiddelen, met name in gevallen waarin het bewaringsbevel tegelijk is uitgevaardigd met een verstrekkingsbevel om gegevens te verkrijgen. Zoals ook door de Groep artikel 29 in haar verklaring is aanbevolen, moeten er rechtsmiddelen worden vastgesteld die ten minste gelijkwaardig zijn aan de middelen die beschikbaar zijn in nationale zaken.

h) Veiligheid van gegevensdoorgiften als aan een bevel wordt voldaan

Volgens de EDPB voorziet de ontwerpverordening alleen in bevelen die gericht moeten worden aan ontvangers binnen de Europese Unie en daardoor niet in specifieke kanalen voor de doorgifte van gegevens tussen adressaten en dienstverleners die buiten de Europese Unie zijn gevestigd.

Hoewel de EDPB toejuicht dat verdere afwijkingen ten opzichte van het algemene Europese kader voor de bescherming van gegevens, afwezig zijn, herinnert hij eraan dat elk bevel aan een adressaat waarbij sprake is van een doorgifte buiten de EU, in overeenstemming moet zijn met het door de AVG geschapen rechtskader. Het rechtskader voor justitiële samenwerking moet ervoor zorgen dat waarborgen voor de bescherming van gegevens worden gerespecteerd. Het omzeilen van deze waarborgen mag er niet ook toe leiden dat adressaten de vereisten voor gegevensdoorgifte bij verstrekkings- of bewaringsbevelen omzeilen om aan deze bevelen te voldoen.

Hoewel de EDPB bovendien toejuicht dat geen verplichting tot het ontsleutelen van versleutelde gegevens wordt opgelegd[35], is hij bezorgd dat de ontwerpvoorstellen niet voorzien in specifieke eisen aan adressaten om de authenticiteit van verstrekte gegevens te beoordelen. Hij onderstreept dat deze beoordeling ook een toegevoegde waarde is van de traditionele instrumenten op basis van justitiële samenwerking en waarschuwt tegen het verhoogde risico voor betrokkenen indien een dergelijke beoordeling niet plaatsvindt.

Conclusies

Op basis van deze beoordeling wil de EDPB de medewetgevers de volgende aanbevelingen doen.

1) Artikel 82, lid 1, VWEU moet niet als rechtsgrondslag van de verordening worden genomen.
2) De noodzaak van een nieuw instrument in het licht van de bestaande EOB-richtlijn of rechtshulpverdragen, moet beter worden onderbouwd met onder andere een gedetailleerde analyse van middelen die minder ingrijpend zijn ten aanzien van grondrechten. Dat kunnen wijzigingen van de bestaande instrumenten zijn of een beperking van het toepassingsgebied van dit instrument wat betreft bewaringsbevelen, gecombineerd met andere bestaande procedures voor het verkrijgen van toegang tot gegevens.
3) De verordening moet voorzien in een langere termijn, die de uitvoerende dienstverlener in staat moet stellen waarborgen voor de bescherming van grondrechten te respecteren.
4) Het beginsel van de dubbele strafbaarheid moet gehandhaafd worden, met name als de locatiecriteria van de gegevens worden losgelaten om de verplichting in stand te houden dat rekening moet worden gehouden met de waarborgen die in beide betrokken staten worden geboden (de staat van de verzoekende autoriteit en de staat waar de dienstverlener is gevestigd).
5) De reikwijdte van de verordening moet beperkt worden tot verwerkingsverantwoordelijken in de zin van de AVG of er moet een bepaling in worden opgenomen dat in het geval waarin de aangezochte dienstverlener niet de verwerkingsverantwoordelijke van de gegevens is, maar de verwerker, de laatstgenoemde de verwerkingsverantwoordelijke moet informeren.
6) De verordening moet waarborgen voor gegevensdoorgiften bevatten voor het geval dat de dienstverlener gevestigd is in een derde land waar op dat vlak geen adequaatheidsbesluit bestaat of moet verwijzen naar Richtlijn (EU) 2016/680 aangezien deze waarborgen van toepassing zijn.
7) Aangezien de verplichte aanwijzing van een wettelijk vertegenwoordiger anders is dan bij de AVG, moet in de verordening worden bepaald dat onderscheid moet worden gemaakt tussen

[35] Zie overweging 19 en bladzijde 240 van de effectbeoordeling.

de wettelijk vertegenwoordiger die is aangewezen overeenkomstig de verordening inzake elektronisch bewijsmateriaal en die welke is aangewezen overeenkomstig artikel 3, lid 2, van de AVG.

8) De verordening moet een bredere definitie van elektronische-communicatiegegevens bevatten om ervoor te zorgen dat de passende waarborgen en voorwaarden voor toegang die moeten worden vastgesteld, ook voor niet-inhoudelijke en inhoudelijke gegevens gelden.
9) De verordening moet drempels opwerpen voor de uitvaardiging van bevelen en bevelen moeten worden uitgevaardigd of goedgekeurd door rechtbanken. Dit geldt niet voor verstrekte abonneegegevens, mits de omschrijving van deze categorie van gegevens sterk is teruggebracht tot zeer basale informatie die net voldoende is om iemand te identificeren zonder communicatiegegevens openbaar te maken.
10) De verordening moet de toegang tot abonneegegevens en toegangsgegevens beperken tot een strikte lijst van strafbare feiten of ten minste tot "ernstige strafbare feiten".
11) De termijn voor het verstrekken van gegevens, met name in noodgevallen, moet in de verordening beter worden verantwoord. Daarnaast moet de mogelijkheid van een versnelde procedure van zes uur de verplichting voor verzoekende autoriteiten inhouden de noodzaak van het gebruik van deze procedure aan te tonen, ook achteraf, om toezicht te kunnen uitoefenen op het gebruik van deze uitzonderlijke bevoegdheden.
12) De procedure die de verstrekking van inhoudelijke gegevens mogelijk maakt, zonder betrokkenheid van de bevoegde autoriteiten van de lidstaat waar de betrokkene zich bevindt, moet worden geschrapt.
13) Waarborgen omtrent de uitvaardiging van Europese bewaringsbevelen in de verordening moeten worden verbeterd.
14) De verordening moet ten minste voorzien in de traditionele afwijkende bepaling dat, indien er gegronde redenen zijn om aan te nemen dat de uitvoering van een bevel in een inbreuk op een grondrecht van de betrokkene zou resulteren en de tenuitvoerleggingsstaat daardoor zijn verplichtingen betreffende de bescherming van de grondrechten die zijn vervat in het Handvest niet zou nakomen, de tenuitvoerlegging van het bevel moet worden geweigerd.
15) De verordening moet voorzien in een bredere verplichting om de bevoegde autoriteiten van een derde land waar de dienstverlener die verzocht is gegevens te verstrekken zich bevindt, te raadplegen in geval van een wetsconflict om subjectieve interpretaties van een enkele rechtbank te voorkomen.
16) De geldigheid en de duur van bewaringsbevelen moeten nauwer verband houden met de bijbehorende verstrekkingsbevelen.
17) De beveiliging van gegevensdoorgiften moet beter worden gewaarborgd.
18) Er moet voor gezorgd worden dat de authenticiteit van de gegevens wordt gecontroleerd, met name indien versleutelde gegevens kunnen worden verstrekt.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)