Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 16/2025 van 27 maart 2025

Betreft: advies uit eigen beweging *betreffende het Verdrag van de Verenigde Naties tegen cybercriminaliteit* (CO-A-2025-019)

Vertaling

Inleiding

In het kader van het goedkeuringsproces van het Verdrag van de Verenigde Naties tegen cybercriminaliteit werd de EDPB verzocht zijn standpunt te herhalen over het belang van de versleuteling van communicatiegegevens. De Autoriteit maakt van deze gelegenheid gebruik om een advies uit eigen beweging over deze kwestie uit te brengen en beveelt aan om, indien de Kamer niet afziet van het verlenen van instemming met de tekst van dit Verdrag, op zijn minst het Hof van Justitie te raadplegen over de verenigbaarheid ervan met het Handvest van de grondrechten.

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"), aanwezig: de dames Cédrine Morlière, Nathalie Ragheno en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name artikel 23 (hierna "WOG");

Gelet op artikel 43 van het Reglement van interne orde volgens hetwelk de beslissingen van de Autorisatie- en Adviesdienst bij meerderheid van stemmen genomen worden;

Gelet op 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* (hierna "AVG");

Voor normatieve teksten die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie zijn de adviezen in principe zowel in het Nederlands als in het Frans beschikbaar op de website van de Autoriteit. De 'Originele versie' is de versie die collegiaal gevalideerd werd.

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Brengt op 27 maart 2025 het volgende advies uit:

I. CONTEXT EN REIKWIJDTE VAN HET ADVIES

1. Het Verdrag van de Verenigde Naties tegen cybercriminaliteit (hierna "het Verdrag") werd op 24 december 2024 aangenomen door de Algemene Vergadering van de Verenigde Naties bij resolutie 79/243[1].

2. Het Verdrag zal openstaan voor ondertekening door de staten tijdens een ceremonie die medio 2025[2] in de stad Hanoi, Vietnam, zal plaatsvinden. Vervolgens kan het worden geratificeerd door de staten die partij zijn, en treedt het in werking zodra 40 staten formeel partij zijn bij het Verdrag[3].

3. Dit Verdrag bestaat uit een preambule en negen hoofdstukken: Algemene bepalingen, Strafbaarstelling, Rechtsmacht, Procedurele maatregelen en rechtshandhaving, Internationale samenwerking, Preventieve maatregelen, Technische bijstand en uitwisseling van informatie, Uitvoeringsmechanisme en Slotbepalingen (vrije vertaling).

4. Verscheidene bepalingen van het Verdrag zijn op tal van punten bekritiseerd[4].

5. Ook verschillende bepalingen met betrekking tot gegevensbescherming zijn problematisch[5] (zoals bijvoorbeeld de bepalingen over de bewaring van communicatiegegevens[6] en de samenwerking tussen

---

[1] Zonder stemming (zie https://unis.unvienna.org/unis/pressrels/2024/uniscp1184.html) en op basis van het verslag van de Derde Commissie (A/79/460, § 15).

[2] De exacte datum is nog niet bekendgemaakt (zie https://www.unodc.org/unodc/en/cybercrime/convention/home.html).

[3] Zie https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

[4] Zie met name

https://www.hrw.org/sites/default/files/media_2023/08/ARTICLE%2019%20and%20Human%20Rights%20Watch%E2%80%99s%20Comments%20on%20the%20Draft%20Text%20of%20the%20UN%20Cybercrime%20Convention_1.pdf; https://www.eff.org/deeplinks/2024/01/joint-statement-proposed-cybercrime-treaty-ahead-concluding-session; https://epicenter.works/fileadmin/user_upload/Open_Letter_of_the_Multistakeholder_Community_to_the_Chair_of_AHC.pdf; https://www.gp-digital.org/news/civil-society-sends-joint-letter-urging-eu-and-member-states-to-withdraw-support-from-rights-harming-un-cybercrime-convention/ en G. Vermeulen, "The growing human rights cost of tackling cybercrime at UN, CoE and EU levels: from unlimiting state control and surveillance to limiting the freedom of information, privacy and procedural rights in criminal matters", in Conferência Internacional Sobre o Crime Organizado, Rio de Janeiro, 2023 (https://biblio.ugent.be/publication/01HJJZDJ41NSTF8SX765MB7W61).

[5] Zie advies 9/2022 van de EDPS van 18 mei 2022.

[6] Wat deze kwestie betreft, verwijst de Autoriteit naar haar adviezen 108/2021 (https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf) en 66/2022 (https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-66-2022.pdf) voor alles wat niet uitdrukkelijk in dit advies wordt vermeld.

autoriteiten op internationaal niveau, waarvan de formulering het risico inhoudt dat Europese waarborgen voor de doorgifte van gegevens kunnen worden omzeild[7]). Bovendien, zoals verschillende ngo's hebben opgemerkt, kan de formulering van artikel 28.4 van het Verdrag – die vergelijkbaar[8] is met die van artikel 19.4 van het Verdrag van Boedapest (aangenomen in 2001 door de lidstaten van de Raad van Europa) – leiden tot een verzwakking van de techniek van end-to-endversleuteling van communicatie. De Autoriteit deelt deze bezorgdheid.

II. ONDERZOEK VAN ARTIKEL 28.4 VAN HET VERDRAG

6. Artikel 28.4 van het Verdrag bepaalt dat "*elke staat die partij is, de nodige wettelijke en andere maatregelen treft* ***om zijn bevoegde autoriteiten te machtigen om eenieder die kennis heeft*** *van de werking van het betrokken informatie- en communicatiesysteem, het informatie- en telecommunicatienetwerk of de onderdelen daarvan, of* ***van de maatregelen die zijn genomen ter bescherming van de daarin opgenomen elektronische gegevens, te gelasten in redelijke mate alle nodige informatie te verstrekken*** (...)" (vertaald door de Autoriteit).

7. Zoals verschillende ngo's hebben opgemerkt, kan deze formulering leiden tot een verzwakking van de techniek van end-to-endversleuteling van communicatie. In de 22e aanbeveling van de Groep op hoog niveau inzake toegang tot gegevens voor doeltreffende rechtshandhaving[9] wordt overigens melding gemaakt van het verzoek van de rechtshandhavingsinstanties tot het verkrijgen van vooraf vastgelegde en rechtmatige toegang tot *leesbare* gegevens, "*in overeenstemming met internationale instrumenten*"[10].

8. Het standpunt van de EDPB over het belang van het behoud van versleuteling wordt herhaald in punt 3 van zijn verklaring 5/2024[11]. De Autoriteit sluit zich volledig aan bij deze verklaring, maar wenst enkele verduidelijkingen aan te brengen in het licht van een mogelijke parlementaire instemming met dit Verdrag.

---

[7] Zie artikel 36.1.c) van het Verdrag, waarin de staten die partij zijn, worden aangemoedigd om "*bilaterale of multilaterale overeenkomsten te sluiten om de doorgifte van persoonsgegevens te faciliteren*" (vertaald door de Autoriteit), zoals opgemerkt door G. Vermeulen, *op. cit.*, slides 6 en 7; zie ook de Civil society's joint letter urging EU and member states to withdraw support from rights-harming UN Cybercrime Convention.

[8] Het Verdrag van Boedapest heeft betrekking op "*IT-systemen*" en "*maatregelen ter bescherming van de computergegevens*", terwijl het voorliggende VN-verdrag betrekking heeft op "*informatie- en communicatiesystemen*" (vrije vertaling).

[9] Zie *Step 3* van de herziene versie van dit verslag die door de Raad aan de delegaties is voorgelegd, 13 maart 2025 (p. 75) https://data.consilium.europa.eu/doc/document/ST-15941-2024-REV-2/en/pdf.

[10] Pp. 14 en 20.

[11] Statement on the recommendations of the High-Level Group on Access to Data for Effective Law Enforcement.

1. Risico op doelafwending

9. Allereerst benadrukt de Autoriteit dat, voordat een bewakingsmaatregel wordt toegestaan, de wetgever zich bewust moet zijn van het feit dat doelafwendingen inherent zijn aan onze technologische samenlevingen – zelfs wanneer men zich bewust is van de risico's. Dergelijke afwendingen doen zich namelijk voor zodra de verleiding bestaat, dat wil zeggen zodra een technologische ontwikkeling het mogelijk maakt gegevens te registreren en te bewaren[12]. Met andere woorden, hoewel de Autoriteit erkent dat sommige maatregelen gerechtvaardigd kunnen zijn, moet men beseffen dat **alleen een algeheel verbod op de bewakingsmaatregel werkelijk effectief is om doelafwendingen te voorkomen**. Een vaak aangehaald voorbeeld is de exponentiële toename van het aantal telefoontaps in de Verenigde Staten na de goedkeuring van de Wiretap Act van 1968, die het afluisteren nochtans beperkte tot de ernstigste gevallen en waarvan de wettelijke waarborgen sinds de goedkeuring ervan voortdurend zijn uitgehold[13].

10. Versleuteling daarentegen staat al sinds het midden van de jaren 1990 in het vizier van politiële autoriteiten[14]. In 1995 zouden telefoons en andere communicatiemiddelen worden gebruikt door drugskartels, terroristen en ontvoerders[15]. In 2014 waarschuwde de directeur van de Amerikaanse FBI voor het risico van "*blindelings werken*" tegenover "*plegers van misdrijven die de meest kwetsbaren onder ons uitbuiten* [,] *... gewelddadige criminelen die het op onze gemeenschappen hebben gemunt*[,] *... een terroristische cel die sociale netwerken gebruikt om mensen te rekruteren, aanslagen te plannen en uit te voeren*"[16] (vertaald door de Autoriteit). In de jaren 2020 beriep de Europese Commissie zich op de noodzaak om de online verspreiding van kindermisbruikmateriaal (CSAM) te voorkomen als reden om zich te verzetten tegen end-to-endversleuteling[17]. Opgemerkt moet worden dat dit laatste initiatief tot zeer heftige reacties leidde vanuit de wetenschappelijke wereld en de EDPS, en dat de Europese Ombudsman tot de conclusie kwam dat er sprake was van wanbeheer door de Europese Commissie[18].

---

[12] Zie de masterproef van M. Jacobs, Function Creep in Surveillance Situations – Identifying control paradoxes through agency and power relations using ANT, 2016 (https://avpn.asia/wp-content/uploads/2020/12/06.pdf).

[13] Over deze kwestie, zie Jennifer S. Granick et al., Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale, 52 Loy. L.A. L. Rev. 431 (2019) (https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=3061&context=llr); opgemerkt dient te worden dat een studie over videobewaking sinds 2007 (datum van de inwerkingtreding van de camerawet) in België waarschijnlijk tot eenzelfde conclusie zou komen.

[14] Voor een gedetailleerde analyse van wat als "crypto war" wordt beschouwd, zie Bart Preneel (2024), The Encryption Debate: An Enduring Struggle. *In* Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24). Association for Computing Machinery, New York, NY, USA, 1–3. https://doi.org/10.1145/3626232.3655998.

[15] Zie https://archive.epic.org/crypto/ban/freeh.html; zie ook de Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer (PB EU nr. C 329 van 04/11/1996 blz. 0001 – 0006).

[16] https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[17] Zie https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance/; de Autoriteit maakt zich dan ook ernstige zorgen wanneer zij in de beleidsverklaring van de minister belast met Digitalisering leest dat België zich op Europees niveau zal blijven inzetten voor de goedkeuring van de CSAM-verordening (https://www.lachambre.be/flwb/pdf/56/0767/56K0767030.pdf, p. 13).

[18] Zie de beslissing van 12 juli 2024 in de zaak 1945/2023/MIG (https://www.ombudsman.europa.eu/nl/decision/nl/189484).

2. Typologie van de verzwakking van versleuteling

11. Zoals de EDPB aangeeft, kan de verzwakking van de bescherming die door versleuteling wordt geboden, voortvloeien uit verschillende technische maatregelen. Deze zijn niet louter beperkt tot de invoering van een "backdoor" in het versleutelingsproces zelf, maar kunnen ook maatregelen omvatten die de waarborgen van versleuteling tenietdoen of aanzienlijk verzwakken (zoals bijvoorbeeld een "*client-side process*" dat toegang op afstand tot gegevens mogelijk maakt voordat deze versleuteld worden of nadat ze door de ontvanger zijn ontsleuteld).

12. Daarnaast zouden aanbieders, om te voldoen aan rechtmatige bevelen tot interceptie of toegang, **technisch verplicht** kunnen worden **om maatregelen te treffen die de versleuteling op een niet-gedifferentieerde manier verzwakken voor alle gebruikers**, zelfs wanneer het oorspronkelijke bevel tot interceptie of toegang beperkt was tot een specifiek individu of een bepaalde groep van individuen (zie de zaak van het EHRM PODCHASOV t. RUSLAND).

13. Meer in het algemeen herinnert[19] de Autoriteit eraan dat:

a) elke nieuwe toegangsmogelijkheid tot informatie (zelfs als deze voor de ordediensten is) de complexiteit van het systeem vergroot, wat betekent dat het gebied dat kwetsbaar is voor aanvallen groter wordt en dus het risico op zwakke plekken toeneemt;
b) de kans dat een dergelijke toegangsmogelijkheid wordt misbruikt door cybercriminelen (of deze nu staatsgebonden zijn of deel uitmaken van een criminele organisatie) zeer groot is;
c) het grote aantal (rechtshandhavings)instanties dat toegang moet kunnen krijgen, nog meer technische en juridische problemen met zich meebrengt.

3. Ongewenste neveneffecten

14. De Autoriteit voegt daaraan toe dat de verzwakking van end-to-endversleuteling paradoxaal genoeg gevolgen kan hebben voor de **nationale veiligheid**. Ter illustratie: de Chinese groep APT (Advanced Persistent Threat) *Salt Typhoon* wist zich toegang te verschaffen tot 9 Amerikaanse aanbieders van telecommunicatiediensten[20], juist omdat er geen gebruik werd gemaakt van end-to-endversleuteling. Hierdoor slaagde de groep erin mogelijk zeer gevoelige communicatie van de Amerikaanse overheid te onderscheppen.

---

[19] In die zin, zie Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner, Keys under doormats: mandating insecurity by requiring government access to all data and communications, *Journal of Cybersecurity*, Volume 1, Issue 1, September 2015, Pages 69–79, https://doi.org/10.1093/cybsec/tyv009.

[20] https://en.wikipedia.org/wiki/2024_United_States_telecommunications_hack.

15. Bovendien stelt de EDPB in zijn verklaring 5/2024 dat het verhinderen van het gebruik van versleuteling of het verzwakken van de doeltreffendheid van de bescherming die deze biedt, **ernstige gevolgen** kan hebben **voor de eerbiediging van de privacy en de vertrouwelijkheid van gebruikers, hun vrijheid van meningsuiting, en de innovatie en de groei van de digitale economie**, die steunt op het hoge niveau van vertrouwen en veiligheid dat deze technologieën bieden.

16. De Autoriteit merkt in dit verband op dat het Verdrag geen **uitzonderingen bevat voor journalisten, mensenrechtenverdedigers en onderzoekers** op het gebied van cyberveiligheid[21]. Nationale wetgeving kan hier uiteraard in voorzien, maar sommige staten zullen hier meer aandacht aan besteden dan andere. **Het zou dan ook betreurenswaardig zijn als België de inwerkingtreding van een verdrag zou goedkeuren waarvan wordt gevreesd dat het zou kunnen worden gebruikt** om de vrijheid van meningsuiting van journalisten en mensenrechtenverdedigers in te perken[22].

17. Voor onderzoekers (zowel in België als in het buitenland) is het ook van essentieel belang dat zij elektronische systemen kunnen bestuderen en op verantwoorde wijze zwakke punten kunnen identificeren, zonder te worden gecriminaliseerd. Daarnaast is het van cruciaal belang dat onderzoekers niet verplicht worden om kwetsbaarheden voortijdig bekend te maken, en dat zwakke punten worden gemeld in het kader van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden[23]. Volgens de Autoriteit dienen in de eerste plaats de onderzoekers zelf en de organisaties die verantwoordelijk zijn voor de betrokken systemen te handelen. De overheid mag pas worden geïnformeerd wanneer de risico's grondig zijn onderzocht en er reeds een eerste inperkingsmaatregel is getroffen[24].

4. Noodzaak en evenredigheid van de maatregel

18. De Autoriteit is van oordeel dat België zich er alleen toe kan verbinden om exploitanten een verzwakking van versleuteling op te leggen "*onder voorbehoud en in de mate waarin het noodzakelijke en evenredige karakter van de maatregel wordt aangetoond*"[25] (vertaald door de Autoriteit). Zoals benadrukt in een verslag aan de Hoge Commissaris van de Verenigde Naties voor de mensenrechten, waarin bezorgdheid wordt geuit over de bedreigingen die toezicht voor democratieën vormt: "*Staten*

---

[21] Over deze kwestie, zie https://cyberscoop.com/un-cybercrime-treaty-threatens-security-research-ilona-cohen-op-ed/.

[22] Zie met name de *hierboven* vermelde brief.

[23] Zie https://ccb.belgium.be/sites/default/files/Brochure_CVDP_FR_1.pdf.

[24] Zie de norm ISO/IEC 29147:2018; opgemerkt moet worden dat de Cyber Resilience Act vanuit dit oogpunt eveneens problematisch is. Onmiddellijke kennisgeving aan de overheid houdt namelijk een risico op misbruik in.

[25] Overeenkomstig artikel 52(1) van het Handvest van de grondrechten van de EU.

verzuimen al te vaak de doeltreffendheid aan te tonen van de toezichtsystemen die zij invoeren."[26] (vertaald door de Autoriteit) Daarom moet de nationale wetgever beschikken over objectieve gegevens[27], waaronder – indien van toepassing – statistieken. In voorkomend geval zou dit moeten leiden tot **een onderscheid naargelang de context waarin toegang tot gegevens wordt overwogen** (gegevens op het apparaat van de gebruiker of op de servers van de aanbieder, vóór of na een inbeslagneming, met of zonder noodzaak tot gegevensexport of realtime toegang tot communicatiegegevens), en dus tot **het bepalen van de toelaatbare omvang van de inmenging**. Dit zou het ook mogelijk moeten maken om de territoriale en temporele **grenzen** van een dergelijke maatregel vast te stellen.

19. De Autoriteit betreurt overigens dat het Verdrag niet vereist dat de staten die partij zijn, statistieken opstellen met het oog op de **publicatie van nationale evaluatieverslagen**. De Autoriteit is van oordeel dat dit moet worden verholpen om te voorkomen dat de staten die partij zijn, kan worden verweten dat zij de doeltreffendheid van de door hen getroffen maatregelen niet aantonen.

5. Vermijden om de verantwoordelijkheid op de aanbieders af te schuiven

20. Tot slot waarschuwt de EDPB in zijn eerdergenoemde verklaring ook voor "*de **verleiding om tegenstrijdige eisen op te leggen aan aanbieders** (zoals het tegelijkertijd mogelijk maken van het onderscheppen van specifieke communicatie en het niet op willekeurige wijze verzwakken van versleuteling), en hen te "verplichten […] om een manier te vinden" om daaraan te voldoen.* (…) *De EDPB adviseert dan ook om te **bepalen en** te **evalueren welke soorten maatregelen** door aanbieders moeten worden getroffen, zodat kan worden beoordeeld of deze maatregelen de versleuteling en de beveiliging van persoonsgegevens en communicatie in het algemeen daadwerkelijk verzwakken. Meer in het algemeen is het van cruciaal belang dat elke aanbeveling die het gebruik van een technische oplossing inhoudt, wordt ondersteund door een beoordeling van de praktische haalbaarheid en de verenigbaarheid van die oplossing met de verplichtingen van privacy by design en privacy by default.* (…)" (vertaald door de Autoriteit)

6. Mogelijkheden voor de Kamer van volksvertegenwoordigers

21. In het besluit van de Raad van de Europese Unie waarbij de Europese Commissie (in 2022)[28] wordt gemachtigd om namens de Europese Unie onderhandelingen over dit verdrag te openen, werd

---

[26] Verslag van 4 augustus 2022, The right to privacy in the digital age, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement, punt 54.

[27] Zie in dit verband ook B. Preneel (2024), *op. cit.*, punt 5: "(…) *there is a lack of verifiable data from the law enforcement side to substantiate their claimed needs for the interception of encrypted communications and the real-time access to data on client devices*".

[28] Overeenkomstig artikel 218(3) van het Verdrag betreffende de werking van de Europese Unie (hierna "VWEU").

gepreciseerd dat de Unie reeds regels had vastgesteld die betrekking hebben op "*sommige*[29]*, maar niet alle elementen die waarschijnlijk in overweging worden genomen om in het* (...) *verdrag* (...) *te worden opgenomen*"[30]. De Raad rechtvaardigt de machtiging met de noodzaak om "*de integriteit van het Unierecht te beschermen en te waarborgen dat de regels van het internationaal recht en het recht van de Unie consistent blijven*"[31]. De Raad herinnert er echter aan dat zijn besluit om de Europese Commissie te machtigen om te onderhandelen "*geen afbreuk* [*mocht*] *doen* (…) *aan de deelname van de lidstaten aan de onderhandelingen* (…) *en aan elk later besluit om een dergelijk verdrag te sluiten, te ondertekenen of te bekrachtigen*"[32].

22. In België hebben verdragen krachtens artikel 167, §§ 2 en 3, van de Grondwet pas interne werking nadat zij **de instemming van de** bevoegde **parlementaire vergadering** hebben verkregen (de Kamer van volksvertegenwoordigers voor wat betreft het federale niveau). De Grondwet vereist niet dat de instemming voorafgaat aan de bekrachtiging[33], maar volgens de rechtsleer verdient het de voorkeur dat de instemming vóór de bekrachtiging plaatsvindt[34].

23. Bovendien, krachtens artikel 218.11 van het VWEU, "**[*kan*] *een lidstaat, het Europees Parlement***, *de Raad of de Commissie* **[...] *het advies inwinnen van het Hof van Justitie over de verenigbaarheid van een voorgenomen overeenkomst met de Verdragen***. *Indien het Hof afwijzend adviseert, kan de voorgenomen overeenkomst niet in werking treden, behoudens in geval van wijziging daarvan of herziening van de Verdragen.*" Dit is wat de Autoriteit aanbeveelt te doen[35] (met dien verstande dat het advies van het Hof ook van invloed zal zijn op artikel 19.4 van het Verdrag van Boedapest).

---

[29] Het gaat om bepaalde richtlijnen in strafzaken, waaronder de CSAM-richtlijn (Richtlijn 2011/93/EU), de instrumenten die zijn aangenomen op het gebied van politiële en justitiële samenwerking in strafzaken, op het gebied van minimale procedurele waarborgen en op het gebied van gegevensbescherming (AVG, Richtlijn 2016/680 oftewel de zogenaamde Richtlijn "Politie en Justitie" en e-Evidence).

[30] 2e overweging; zie ook de artikelen 82(1) en (2) en artikel 83(1) van het VWEU.

[31] 4e overweging.

[32] 6e overweging.

[33] In tegenstelling tot artikel 12 van het samenwerkingsakkoord van 8 maart 1994 tussen de Federale Overheid, de Gemeenschappen en de Gewesten over de nadere regelen voor het sluiten van gemengde verdragen (MB 6.03.1996).

[34] Zie Ch. Behrendt, La ratification des traités internationaux, une perspective de droit comparé (Belgique), Service de recherche du Parlement européen, p. 27.

(https://www.europarl.europa.eu/RegData/etudes/STUD/2020/646197/EPRS_STU(2020)646197_FR.pdf); zie ook M. UYTTENDAELE, Précis de droit constitutionnel belge, Bruxelles, Bruylant, 2001, p. 880, waarin wordt gepreciseerd dat dit zo is "*om een conflict tussen de wetgevende en de uitvoerende macht te voorkomen en om te voorkomen dat er een verschil ontstaat tussen de bindende kracht van het verdrag in de internationale rechtsorde en in de interne rechtsorde*" (vertaald door de Autoriteit).

[35] Zoals dit overigens ook voorafgaand aan de aanneming van het Tweede aanvullend protocol bij het Verdrag van de Raad van Europa inzake cybercriminaliteit had moeten gebeuren, dat met enige haast werd aangenomen, juist om de wedloop tegen het VN-ontwerp van een Russisch-Chinees verdrag niet te verliezen, en waarbij het Europees Parlement werd meegedeeld dat het ging om een ontwerp dat "*gunstig is voor de voorbereiding van prioritaire wetgevingsdossiers voor Spanje, zoals "CSAM"*" (vertaald door de Autoriteit) (zie de stemverklaring van Juan Fernando López Aguilar in de LIBE-commissie van het Europees Parlement (A9-0002/2023)); voor een vergelijking tussen het Verdrag van Boedapest en het VN-verdrag tegen cybercriminaliteit, zie https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime.

24. Zoals hierboven vermeld, zijn echter talrijke bepalingen van het Verdrag die geen betrekking hebben op gegevensbescherming, bekritiseerd. Indien de overheid zou overwegen een wetsontwerp ter goedkeuring van dit Verdrag in te dienen, beveelt de Autoriteit aan om **de tekst**, alvorens het wetsontwerp ter goedkeuring aan de Kamer voor te leggen, voor advies **voor te leggen** aan het **Federaal Instituut voor de Rechten van de Mens**.

OM DEZE REDENEN,

De Autoriteit is van oordeel dat,

- **in hoofdzaak** geen instemming mag worden verleend aan het Verdrag van de Verenigde Naties tegen cybercriminaliteit;
- **subsidiair**, zoals bepaald in artikel 218.11 van het VWEU, de Kamer van volksvertegenwoordigers het Hof van Justitie van de Europese Unie dient te verzoeken — en/of haar tegenhangers in het Europees Parlement dient te vragen het Hof te verzoeken — te beoordelen of het Verdrag (en met name artikel 28.4 daarvan) verenigbaar is met de verdragen en in het bijzonder met de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie, en haar instemming met het Verdrag dient uit te stellen in afwachting van het advies van het Hof.

Voor de Autorisatie- en Adviesdienst,
(get.) Cédrine Morlière, Directeur