



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 77/2024 van 23 augustus 2024

Betreft: adviesaanvraag met betrekking tot een wetsontwerp *betreffende de weerbaarheid van kritieke entiteiten* (CO-A-2024-205)

Trefwoorden: kritieke entiteiten – OCAD – sectorale overheden – mededeling van gegevens – veiligheidsverificatie – SICAD

Vertaling

Inleiding

Het advies betreft een wetsontwerp tot omzetting van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad betreffende de weerbaarheid van kritieke entiteiten.

De Autoriteit wijst voornamelijk op het gebruik van onduidelijke begrippen zoals "*nuttige informatie*" of "*enig andere overheid*" en het gebrek aan objectieve elementen om te bepalen welke personen aan een veiligheidsverificatie kunnen worden onderworpen of wanneer gegevens geldig kunnen worden meegedeeld aan een gefedereerde entiteit.

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig: mevrouw Juline Deschuyteneer, mevrouw Cédrine Morlière, mevrouw Nathalie Ragheno en mevrouw 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 de artikelen 23 en 26 (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 worden aangenomen;

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");

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

Gelet op de adviesaanvraag van mevrouw Annelies Verlinden, minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing (hierna "de aanvrager"), ontvangen op 6 juni 2024;

Gelet op de aanvullende informatie ontvangen op 19 juni 2024;

Brengt op 23 augustus 2024 het volgende advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De aanvrager heeft het advies van de Autoriteit gevraagd over een wetsontwerp betreffende de weerbaarheid van kritieke entiteiten (hierna "het ontwerp") en meer in het bijzonder de artikelen 8, 16, 19, 20, 23, 24 en 63.
2. In de memorie van toelichting staat dat het ontwerp tot doel heeft Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad betreffende de weerbaarheid van kritieke entiteiten om te zetten¹.

II. ONDERZOEK VAN HET ONTWERP

1) Dreigingsanalyse door het OCAD (artikel 8) en informatie-uitwisseling (artikel 23)

3. Krachtens artikel 8 in ontwerp moet het OCAD uiterlijk om de vier jaar een gemeenschappelijke strategische evaluatie² (hierna "*dreigingsanalyse*") uitvoeren voor de sectoren en deelsectoren die zijn vermeld in de bijlage van het ontwerp. Daartoe verplicht artikel 8, § 3, in ontwerp de autoriteit die door de Koning is aangewezen als "*Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten*", de sectorale overheden³ (zoals het BIPT, de Nationale Bank of het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten), de inlichtingen- en veiligheidsdiensten, de politiediensten, de Administratie der Douane en Accijnzen, de FOD Mobiliteit en Vervoer, de Dienst Vreemdelingenzaken, de FOD Buitenlandse Zaken, de Algemene Directie Crisiscentrum, het directoraat-generaal Penitentiaire Inrichtingen, de dienst Erediensten en Vrijzinnigheid, de Algemene Administratie van de Thesaurie en de door de Koning op voorstel van de Nationale Veiligheidsraad aangewezen overheidsdiensten⁴ om "*nuttige informatie*" mee te delen aan het OCAD.
4. Wat de maatregelen met een impact op gegevensbescherming betreft, heeft het ontwerp twee belangrijke gevolgen:

¹ Voor een historische analyse van de wetgeving inzake kritieke infrastructures en in het bijzonder de zogenaamde "CER"-richtlijn, die het ontwerp beoogt om te zetten, zie Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85–101. <https://doi.org/10.1080/23789689.2022.2128562>

² Als bedoeld in artikel 8, eerste lid, 1°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging (BS 20.07.2006).

³ Vermeld in de bijlage van het ontwerp (en, in voorkomend geval, nog aan te wijzen bij KB).

⁴ Met andere woorden, de ondersteunende diensten van het OCAD vermeld in artikel 2, eerste lid, 2°, van de voormelde wet betreffende de analyse van de dreiging.

- 1) het voegt nieuwe soorten dreigingen toe aan de opdrachten van het OCAD⁵ en bijgevolg nieuwe doeleinden voor de mededeling en verwerking van gegevens; en
- 2) het breidt de lijst uit van de diensten, andere dan de ondersteunende diensten, die verplicht zijn om "nuttige informatie" mee te delen.

Mededeling van nuttige informatie aan het OCAD

5. De Autoriteit wijst er in de eerste plaats op dat de **overheidsdiensten die door de Koning kunnen worden aangewezen, op zijn minst moeten kunnen worden bepaald** op basis van hun wettelijke opdrachten. Artikel 8 moet in die zin dus worden geherformuleerd en er moet worden aangetoond dat het noodzakelijk en evenredig is om die extra ondersteunende diensten op te nemen.
6. Voorts merkt de Autoriteit op dat het begrip "*nuttige informatie*" in artikel 8, § 3, wordt vervangen door "*relevante informatie*" in het commentaar bij die bepaling. In het commentaar bij artikel 8 staat alleen dat dergelijke informatie "*[...] onder meer de incidentenmeldingen door kritieke entiteiten [kan] inhouden*".
7. In dit verband moet eraan worden herinnerd dat het OCAD niet is opgericht als inlichtingendienst. Met andere woorden, het is niet de taak van het OCAD om rechtstreeks informatie te verzamelen. Informatie wordt hem verstrekt door zijn ondersteunende diensten. De opdracht voor het maken van dreigingsanalyses werd in het leven geroepen na een aanslag op de synagoge van Brussel in 1982 en werd toen toevertrouwd aan de Antiterroristische Gemengde Groep (AGG), die deel uitmaakte van de diensten van de rijkswacht⁶ (het idee, dat even werd geopperd, om deze dienst op het terrein actief te laten zijn, werd al "snel verlaten"⁷). De AGG had echter problemen met de informatiedoorstroming⁸.
8. Na de aanslagen van 11 september 2001 werden overal in de wereld nieuwe coördinatiestructuren op poten gezet⁹. Het is in die geest dat "*[...] het ministerieel Comité voor inlichting en veiligheid [op 10 november 2004 besliste] dat de A.G.G. effectief omgevormd zou worden tot een orgaan, waarbij alle voor een dreigingevaluatie pertinente inlichtingen moeten samenkomen en waarin die gegevens*

⁵ Hiermee wordt de tendens voortgezet die werd ingezet door de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (BS 15 juli 2011).

⁶ T. Coosemans, "Les dispositifs de sécurité avant et après le 11 septembre 2001", *Courrier hebdomadaire*, CRISP, nr. 1762-1763, 2002, blz. 32 (enkel beschikbaar in het Frans).

⁷ W. Van LAETHEM, "Het coördinatieorgaan voor de dreigingsanalyse: een punctuele analyse", *Vigiles*, 2007/4, blz. 110, noot 6.

⁸ T. Coosemans, "Les dispositifs de sécurité avant et après le 11 septembre 2001", *op. cit.*, blz. 31 (enkel beschikbaar in het Frans); K. Lasoen, "Indications and Warning in Belgium: Brussels is not Delphi", *Journal of Strategic Studies*, volume 40, nr. 7, 2017, blz. 932.

⁹ Zie W. Van LAETHEM, "Het coördinatieorgaan voor de dreigingsanalyse", *op. cit.*, blz. 111.

geanalyseerd en verwerkt kunnen worden"¹⁰. Die beslissing leidde tot de goedkeuring van de wet van 10 juli 2006 betreffende de analyse van de dreiging¹¹.

9. De Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), de rechtsvoorganger van de GBA, bracht advies nr. 8/2005¹² uit over dat wetsvoorstel. Daarbij merkte de CBPL – net als de afdeling Wetgeving van de Raad van State¹³ – reeds de volgende zaken op:

- "het **begrip "relevantie" wordt niet gedefinieerd** in de tekst¹⁴;
- de **risico's die ontstaan wanneer aan verantwoordelijken voor de verwerking verplichtingen opgelegd worden die niet tot hun basisopdrachten behoren**¹⁵;
- de Commissie stelt zich meer in het bijzonder vragen bij het **vaststellen van de criteria** op basis waarvan de deelnemende diensten zullen beoordelen of een informatie relevant is¹⁶;
- bij gebrek aan **duidelijke richtlijnen**, dreigt men uit te monden in een zeer uitgebreide doorgifte van informatie in die zin dat een dienst, om niet gestraft te worden, veeleer zal verkiezen te veel, in plaats van te weinig informatie door te geven, hetgeen ondermeer zou leiden tot een **schending van het principe inzake proportionaliteit** zoals dit voorzien is door de wet op de bescherming van de persoonlijke levenssfeer¹⁷;
- het CODA (sic) [moet] zo nauwkeurig mogelijk [...] bepalen welke verwerkingen zij (sic) wenst uit te voeren zodat de deelnemende diensten over **duidelijke richtlijnen** beschikken aangaande de relevantie van de informatie die zij geacht worden door te geven¹⁸;
- het [is] onontbeerlijk [...] dat de informatie kan getraceerd worden (van wie is zij afkomstig, aan wie werd zij doorgegeven, enz.) en dat een controle a posteriori zou worden voorzien voor alle deelnemende overheden van het CODA (sic) wat betreft de relevantie van het doorgeven van deze informatie¹⁹.

¹⁰ *Ibidem*, blz. 112.

¹¹ BS 20.07.2006.

¹² Advies van 25 mei 2005, Parl. St. Kamer, 17 oktober 2005, 51-2032/001, blz. 90 (<https://www.lachambre.be/FLWB/PDF/51/2032/51K2032001.pdf>).

¹³ Advies nr. 38.782/2/V van 11 augustus 2005, Parl. St. Kamer, 17 oktober 2005, 51-2032/001, blz. 63.

¹⁴ Punt 10, blz. 94.

¹⁵ Advies nr. 33 van 13 december 1999 betreffende wetsontwerpen inzake informaticacriminaliteit, blz. 9 en 10; advies uit eigen beweging nr. 44/2001 van 12 november 2001 betreffende de verenigbaarheid van het onderzoek naar overtredingen van het auteursrecht op het internet met de wetsbepalingen tot bescherming van persoonsgegevens en van telecommunicatie, blz. 6; advies nr. 8/2005 (punt 11, blz. 94) preciseert bovendien dat "hoewel het opzoeken, analyseren en verwerken van informatie met het oog op het verzekeren van de veiligheid van de Staat, van de burger en het bewaren van de openbare orde, behoort tot de wettelijke opdrachten van de inlichtingen- en politiediensten, dit niet zo is voor de andere leden van het CODA (sic) (de "deelnemende diensten") wier wettelijke opdrachten van een heel andere orde zijn. Welnu, het voorontwerp eist van deze diensten een eerste analyse van de informatie aangaande de bestaande of mogelijke dreiging voor de veiligheid van de Staat".

¹⁶ *Op. cit.*, punt 12.

¹⁷ *Ibidem*, punt 12.

¹⁸ *Ibidem*, punt 13.

¹⁹ *Ibidem*, punt 13, blz. 96.

10. In antwoord op die adviezen preciseert de parlementaire voorbereiding van de wet van 2006 dat de regering niet akkoord gaat met de opmerking dat het gebrek aan nauwkeurigheid het risico inhoudt dat de bepaling als onevenredig wordt beschouwd. "*Zij wenst er op te wijzen dat **het in deze 'slechts' gaat om een overdracht aan een andere publieke overheid van reeds wettig verzamelde gegevens. Verder **betreft de overdracht dikwijls geen persoonsgegevens** maar voornamelijk gebeurtenissen. Belangrijker is evenwel dat deze gegevens door OCAM (sic) niet worden gebruikt om individuele beslissingen bvb. van administratieve of gerechtelijk aard, ten aanzien van concrete personen te nemen, maar wel om dreigingsanalyses te maken***".
11. Die precisering – waaraan beter nog eens kan worden herinnerd bij de voorbereidende werkzaamheden van het ontwerp – bevestigt dat het niet de taak van het OCAD is om rechtstreeks informatie (laat staan persoonsgegevens) te verzamelen. Diensten met de status van ondersteunende dienst zijn immers onderworpen aan een wettelijke verplichting om inlichtingen mee te delen. Er moet worden opgemerkt dat die verplichting als ongekend werd gekwalificeerd, aangezien de Europese tegenhangers van het OCAD hier geen aanspraak op kunnen maken²⁰.

Uitbreiding van de autoriteiten die verplicht zijn om informatie mee te delen

12. Door de politie- en inlichtingendiensten, de andere ondersteunende diensten en de sectorale overheden waartoe de mededelingsverplichting wordt uitgebreid, in eenzelfde bepaling betreffende de mededelingsverplichting²¹ op te nemen, creëren de opstellers van het ontwerp het risico op verwarring over de omvang van de verplichting voor elk van hen.
13. De mededelingsverplichting voor de ondersteunende diensten is immers zowel proactief als reactief (tenzij er een embargo is)²² en kan gericht zijn op bijzondere categorieën van gegevens²³. Daarentegen is het niet de taak van de sectorale overheden (zoals het BIPT, de Nationale Bank of het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten) om bij de betrokken entiteiten persoonsgegevens te verzamelen voor een doeleinde dat verband houdt met de bestrijding van terroristische dreigingen, en al helemaal niet om bijzondere categorieën van gegevens in de zin van artikel 9.2. van de AVG te verzamelen.

²⁰ C. THOMAS, "L'organisation fédérale de la lutte antiterroriste en Belgique", Courrier hebdomadaire du CRISP 2020/18-19 (nr. 2463-2464), blz. 79 (enkel beschikbaar in het Frans).

²¹ Met name artikel 8, § 3, van het ontwerp.

²² Zie artikel 6 en [HOOFDSTUK IV](#) van de wet van 2006; Het toepassen van dezelfde regeling op de politie- en inlichtingendiensten als op de andere ondersteunende diensten valt buiten de bevoegdheid van de Autoriteit in het kader van dit advies; voor een kritische bespreking van de tekst van die bepaling zie advies nr. 184/2021 van 4 oktober 2021, punten 40 en volgende (<https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-184-2021.pdf>) en W. Van LAETHEM, "Het coördinatieorgaan voor de dreigingsanalyse", *op. cit.*, blz. 116 en volgende.

²³ Artikel [142](#) WVG.

14. Daarom moet in het ontwerp worden vermeld dat de mededelingsverplichting voor de sectorale overheden (en in het bijzonder met betrekking tot persoonsgegevens) zich beperkt tot de **mededeling van gegevens die uitdrukkelijk door het OCAD zijn opgevraagd en die zij in het kader van hun opdrachten reeds in hun bezit hebben**. De Autoriteit is overigens van oordeel dat in het commentaar bij het desbetreffende artikel moet worden gepreciseerd dat elke poging van een sectorale overheid om zich om te vormen tot een onderzoeksdienst of om spontaan persoonsgegevens met betrekking tot een mogelijke verdenking aan het OCAD²⁴ mee te delen, noodzakelijkerwijs als een onevenredige gegevensverwerking en dus als onrechtmatig zou worden beschouwd.

"Nuttige" informatie maar "noodzakelijke" persoonsgegevens

15. Ten slotte, met betrekking tot de persoonsgegevens waarvan het OCAD kan vragen dat ze worden meegedeeld, herinnert de Autoriteit aan haar advies nr. 34/2024²⁵, waarin zij benadrukt dat het noodzakelijkheids criterium in aanmerking moet worden genomen om te bepalen of gegevens mogen worden verwerkt. *"En de noodzaak om gegevens te verwerken zal in concreto worden beoordeeld in het licht van het doel van de verwerking en de fase waarin de betreffende taak wordt uitgevoerd (de noodzaak van een gegeven kan variëren afhankelijk van de inlichtingencyclus; met name het feit dat een gegeven niet langer nodig is in een latere fase waarin de betreffende taak wordt uitgevoerd, betekent niet dat het in de beginfase niet nodig was)"*.
16. De Autoriteit is dus van oordeel dat, zoals reeds is bepaald in de meest recente bepalingen die van toepassing zijn op de inlichtingendiensten²⁶, artikel 8, § 3, in ontwerp moet worden gewijzigd om te bepalen dat *"wat persoonsgegevens betreft, de mededelingsverplichting ten aanzien van het OCAD uitsluitend betrekking heeft op de gegevens die het OCAD nodig heeft om een dreigingsanalyse uit te voeren"* (en niet op nuttige of relevante informatie).
17. Dezelfde opmerking geldt voor de uitwisseling van *"alle nuttige informatie voor het nemen van externe beschermingsmaatregelen voor de kritieke entiteiten"*, bedoeld in artikel 23 in ontwerp.

2) Mededeling van de dreigingsanalyse door het OCAD aan de sectorale overheden (artikel 8, § 4)

²⁴ In plaats van aan het parket of de politiediensten.

²⁵ Uitgebracht op 15 april 2024 in verband met het wetsvoorstel tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten, punt 28.

²⁶ Zoals artikel [108](#) WVG.

18. Artikel 8, § 4, bepaalt dat het OCAD de dreigingsanalyse meedeelt aan de sectorale overheden. Het doeleinde van die mededeling is de sectorale overheden in staat te stellen die conclusies op te nemen in de risicoanalyse die zij moeten uitvoeren.
19. De Autoriteit veronderstelt dat de door het OCAD meegedeelde conclusies **geen persoonsgegevens bevatten** over daders of verdachten, afkomstig van de ondersteunende diensten²⁷. Als dat wel het geval is, moet dit worden gepreciseerd.
20. **Indien de meegedeelde conclusies toch persoonsgegevens bevatten**, moet het ontwerp grondig worden herzien, waarbij de noodzaak en evenredigheid van een dergelijke mededeling moet worden aangetoond en de essentiële elementen van de registratie van die gegevens door de sectorale overheden moeten worden bepaald. Die bepaling zou moeten worden opgenomen in de verschillende organieke wetten van die sectorale overheden, maar het zou wenselijk zijn om naar die bepalingen te verwijzen in de voorbereidende werkzaamheden van dit ontwerp. In voorkomend geval moet bovendien worden gepreciseerd dat, behalve in naar behoren gemotiveerde uitzonderlijke gevallen, alleen een gepseudonimiseerde versie van de conclusies aan de sectorale overheden zal worden meegedeeld.

3) Contactpunt kritieke entiteit (artikel 16)

21. Artikel 16, § 1, tweede lid, in ontwerp bepaalt dat het contactpunt kritieke entiteit de functie van contactpunt uitoefent ten aanzien van een reeks opgesomde autoriteiten en van "*elke andere bevoegde overheid of openbare dienst voor elke vraag in verband met de weerbaarheid van de entiteit en zijn infrastructuur*".
22. De Autoriteit herinnert eraan dat, tenzij de mededeling van persoonsgegevens van bij de ondersteunende diensten en het OCAM bekende daders of verdachten wordt uitgesloten van de rol van contactpunt, het aantal mogelijke ontvangers van die gegevens een zeer belangrijke impact heeft op de inmenging in de rechten en vrijheden van de betrokkenen. **Het is daarom van essentieel belang dat de lijst van ontvangers en de doeleinden van de mededelingen voldoende nauwkeurig worden bepaald, zodat een verwerkingsverantwoordelijke kan beoordelen of een (verzoek om) mededeling van dergelijke categorieën van gegevens aan een bepaalde burgemeester of andere overheid wel degelijk een wettelijke grondslag heeft en noodzakelijk is.**

²⁷ Indien nodig vindt de mededeling van persoonsgegevens aan de directie van een kritieke entiteit immers plaats via het parket of de politiediensten en niet via het OCAD.

23. Artikel 16 in ontwerp moet daarom worden gewijzigd om te preciseren, **ofwel** dat persoonsgegevens van daders of verdachten die bekend zijn bij de ondersteunende diensten en het OCAD in geen geval aan het contactpunt worden meegedeeld, **ofwel** welke categorieën van persoonsgegevens kunnen worden meegedeeld, door wie, voor welk doeleinde, met inachtneming van welke maximale bewaartermijn, enz. Met andere woorden, in dat tweede geval moeten, naast de noodzaak en evenredigheid van de verwerking, alle essentiële elementen met betrekking tot die verwerking in het ontwerp worden vastgelegd.

4) Opstart van een veiligheidsverificatie door de kritieke entiteiten (artikel 19)

24. Krachtens artikel 19 in ontwerp kan een kritieke entiteit om een antecedentenverificatie²⁸ verzoeken voor de uitoefening van een beroep, functie, opdracht of mandaat, of voor de toegang tot haar lokalen, gebouwen of terreinen.
25. In het commentaar bij die bepaling staat dat "*het risico bestaat dat werknemers van kritieke entiteiten of hun contractanten bijvoorbeeld hun toegangsrechten misbruiken om binnen de organisatie van de kritieke entiteit schade te veroorzaken*".
26. Hoewel het doeleinde van die verwerking als voldoende specifiek, welbepaald en gerechtvaardigd moet worden beschouwd, neemt dit niet weg dat het **personele toepassingsgebied** onvoldoende nauwkeurig is vastgesteld om een verwerkingsverantwoordelijke in staat te stellen te bepalen voor welke categorieën van personen een dergelijke verificatie noodzakelijk en evenredig is en in welke gevallen een verzoek in geen geval kan worden toegestaan.
27. De Autoriteit herinnert er overigens aan dat, door in een "*mogelijkheid*" van een verzoek om verificatie te voorzien, een verwerkingsverantwoordelijke alleen aansprakelijk kan worden gesteld als een dergelijk verzoek wordt gedaan wanneer een dergelijke verwerking niet noodzakelijk en evenredig is voor de beoogde doeleinden. Daarentegen kan een verwerkingsverantwoordelijke die ervan afziet om een dergelijke verificatie te vragen, niet aansprakelijk worden gesteld. Om die verwerking aan de wettelijke verplichting²⁹ te onderwerpen, moet ervoor worden gezorgd dat bij de herformulering van artikel 19 wordt bepaald dat om een dergelijke verificatie "*moet*" worden verzocht.

²⁸ Als bedoeld in artikel [22quinquies](#) van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst (BS 7.05.1999).

²⁹ Voor de goede orde preciseert de Autoriteit dat een wettelijke verplichting niet inhoudt dat modalisering uitgesloten is.

28. De Autoriteit is daarom van oordeel dat artikel 19 in ontwerp zodanig moet worden geherformuleerd dat **objectief wordt bepaald welke categorieën van personen** (op basis van hun taken of andere elementen die moeten worden beschreven) kunnen worden onderworpen aan een veiligheidsverificatie en **op welk moment dat verzoek kan worden gedaan** (vóór de indiensttreding, periodiek, na een gebeurtenis die moet kunnen worden bepaald bij de lezing van het ontwerp en het desbetreffende commentaar?)³⁰.

5) Informatieplicht bij een gebeurtenis (artikel 20)

29. Krachtens artikel 20 in ontwerp moeten de kritieke entiteiten drie autoriteiten **informer**, waaronder de Informatie- en Communicatiedienst van de Federale Politie op het niveau van het gerechtelijk arrondissement³¹ (hierna **de "SICAD"**), wanneer een gebeurtenis plaatsvindt.
30. Onverminderd de eventuele opmerkingen van het COC hierover, is de Autoriteit van oordeel dat de **aanwijzing van de SICAD in plaats van een territoriaal bevoegde bestuurlijke politieoverheid naar behoren moet worden gemotiveerd** in het commentaar bij de desbetreffende bepaling. De Autoriteit maakt van de gelegenheid gebruik om erop te wijzen dat indien, hypothetisch gesproken, de formulering van artikel 20 was gekozen om een technische realiteit te weerspiegelen (bijvoorbeeld omdat de diensten onder de verantwoordelijkheid van de provinciegouverneurs niet over een vergelijkbare infrastructuur beschikken), het passend zou zijn om de techniek aan te passen aan de normen betreffende de vaststelling van de bevoegdheden van de autoriteiten en niet om de normen aan te passen aan een bestaande technische oplossing.

6) Informatie-uitwisseling met de gefedereerde entiteiten (artikel 24, § 2)

31. Artikel 24, § 2, in ontwerp bepaalt dat de sectorale overheid³² (zoals het BIPT, de Nationale Bank of het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten), de autoriteit die door de Koning is aangewezen als "*Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten*" en de kritieke entiteit "*[...] in voorkomend geval, informatie [kunnen] uitwisselen met de gefedereerde entiteiten, voor de kritieke entiteiten die onder hun bevoegdheid vallen*".

³⁰ Zie over deze kwestie ook de formele opmerkingen van de EDPS over het voorstel voor een richtlijn betreffende de veerkracht van kritieke entiteiten, uitgebracht op 11 augustus 2021, blz. 3 in de Franse versie (https://www.edps.europa.eu/system/files/2021-08/21-08-11_edps_comments_critical_entities_fr.pdf, blz. 2 in de Engelse versie (www.edps.europa.eu/system/files/2021-08/21-08-11_edps_comments_critical_entities_en.pdf).

³¹ Als bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

³² Vermeld in de bijlage van het ontwerp (en, in voorkomend geval, nog aan te wijzen bij KB).

32. Voor zover die uitwisselingen persoonsgegevens bevatten, is de Autoriteit van oordeel dat de formulering van een bepaling die een basis kan vormen voor mededelingen aan gefedereerde entiteiten veel nauwkeuriger moet zijn.
33. In elk geval kan de loutere aanwezigheid van een kritieke entiteit (zoals de zetel van een bank of een levensmiddelenbedrijf) op het grondgebied van een gewest de mededeling van persoonsgegevens aan de gewestelijke overheden niet rechtvaardigen. Bovendien, als de gefedereerde entiteit verantwoordelijk is voor de verwerking van de kritieke entiteit, is er strikt genomen geen sprake van mededeling van gegevens, in de zin van de AVG, tussen de kritieke entiteit en de gefedereerde entiteit.
34. Bijgevolg moet, voor zover de informatie-uitwisseling een mededeling van persoonsgegevens inhoudt, artikel 24, § 4, worden geherformuleerd om **die mededeling preciezer te regelen en om het mogelijk te maken de gevallen vast te stellen waarin een mededeling van gegevens als onrechtmatig zou moeten worden beschouwd**. Er moet worden opgemerkt dat als de informatie-uitwisseling verplicht en/of wederkerig zou zijn, een dergelijke uitwisseling alleen rechtmatig zou kunnen plaatsvinden na het sluiten van een samenwerkingsakkoord.

7) Wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (artikel 63)

35. Artikel 63 voegt in de wet van 10 juli 2006 betreffende de analyse van de dreiging een mededelingsverplichting in voor de ondersteunende diensten van het OCAD³³ met betrekking tot de bijzondere categorieën van gegevens³⁴ en de informatie waarover zij in het kader van hun wettelijke opdrachten beschikken en die relevant blijkt met het oog op de verwezenlijking van de doelstellingen van de dreigingsanalyse bedoeld in artikel 8, § 2 (hierboven besproken).
36. De Autoriteit is van oordeel dat de verwijzing naar artikel [142](#) WVG hier ontoereikend is. Daarentegen moet **de gegevensbank** waarin de gegevens worden geregistreerd, worden **geregeld**. Wat de gemeenschappelijke gegevensbank betreft, moet worden verwezen naar de relevante bepalingen en moet worden gepreciseerd welke maatregelen zullen worden genomen om te voorkomen dat irrelevante gegevens worden meegedeeld aan de andere deelnemende diensten. Met andere woorden,

³³ Met name aan de inlichtingen- en veiligheidsdiensten, de politiediensten, de Administratie der Douane en Accijnzen, de FOD Mobiliteit en Vervoer, de Dienst Vreemdelingenzaken, de FOD Buitenlandse Zaken, de Algemene Directie Crisiscentrum, het directoraat-generaal Penitentiaire Inrichtingen, de dienst Erediensten en Vrijzinnigheid, de Algemene Administratie van de Thesaurie.

³⁴ Meer in het bijzonder de "persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook genetische en biometrische gegevens, gezondheidsgegevens, gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen".

er moeten maatregelen worden genomen om te voorkomen dat bijvoorbeeld godsdienstige overtuigingen die door de dienst Erediensten worden meegedeeld, toegankelijk worden gemaakt voor de CFI. Als de mededeling via een andere gegevensbank gebeurt, moet voor die verwerking hetzelfde model gelden als voor de gemeenschappelijke gegevensbank. In voorkomend geval moet rekening worden gehouden met haar advies nr. 97/2023³⁵ bij het opstellen van de bepalingen betreffende de uitwisseling van inlichtingen tussen de ondersteunende diensten en het OCAD.

OM DEZE REDENEN,

De Autoriteit

is van oordeel dat:

- artikel 8 moet worden geherformuleerd zodat de overheidsdiensten die door de Koning kunnen worden aangewezen, kunnen worden bepaald op basis van hun wettelijke opdrachten, en in het commentaar moet worden aangetoond dat het noodzakelijk en evenredig is om die extra ondersteunende diensten op te nemen (punt 5);
- het feit dat het slechts gaat om een overdracht aan een andere publieke overheid van reeds wettig verzamelde gegevens en dat die overdracht dikwijls geen persoonsgegevens betreft, in het commentaar bij de artikelen 8 en 23 moet worden herhaald (punten 10 en 17);
- in het ontwerp moet worden vermeld dat "de mededelingsverplichting voor de sectorale overheden (met betrekking tot persoonsgegevens) zich beperkt tot de mededeling van gegevens die uitdrukkelijk door het OCAD zijn opgevraagd en die zij in het kader van hun opdrachten reeds in hun bezit hebben" en dat in het commentaar bij het desbetreffende artikel moet worden gepreciseerd dat elke poging van een sectorale overheid om zich om te vormen tot een onderzoeksdienst of om spontaan persoonsgegevens met betrekking tot een mogelijke verdenking aan het OCAD mee te delen, noodzakelijkerwijs als een onevenredige gegevensverwerking en dus als onrechtmatig zou worden beschouwd (punten 14 en 17);
- artikelen 8, § 3, en 23 in ontwerp moeten worden gewijzigd om te bepalen dat "*wat persoonsgegevens betreft, de mededelingsverplichting ten aanzien van het OCAD uitsluitend betrekking heeft op de gegevens die het OCAD nodig heeft om een dreigingsanalyse uit te voeren*" (punten 16 en 17);
- artikel 8, § 4, moet worden geherformuleerd (punten 18 tot en met 20);
- de lijst van ontvangers en de doeleinden van de mededelingen nauwkeuriger moeten worden bepaald (punten 22 en 23);

³⁵ Advies van 16 juni 2023 met betrekking tot een voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt.

- artikel 19 zodanig moet worden geherformuleerd dat objectief wordt bepaald welke categorieën van personen kunnen worden onderworpen aan een veiligheidsverificatie en op welk moment dat verzoek kan worden gedaan (punten 27 en 28);
- de aanwijzing van de SICAD naar behoren moet worden gemotiveerd (punt 30);
- artikel 24, § 4, moet worden geherformuleerd om die mededeling preciezer te regelen (punten 32 tot en met 34);
- de gegevensbank waarin de gegevens worden geregistreerd, moet worden geregeld (punt 36).

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