

**Advies van de Raad van het BIPT
van 2 oktober 2026
over
betreffende
de voorontwerpen van wet betreffende
1° het administratief verbod van de activiteiten van
rechtspersonen, vennootschappen zonder
rechtspersoonlijkheid en feitelijke verenigingen of
groeperingen die een ernstige en actuele bedreiging
vormen voor de nationale veiligheid en
2° de beroepen bij de Raad van State tegen de
administratieve verbodsmaatregelen waarin is voorzien
bij de wet van XXX betreffende het administratief
verbod op de activiteiten van bepaalde entiteiten die
een ernstige en actuele bedreiging vormen voor de
nationale veiligheid**

INHOUDSOPGAVE

1.	Voorwerp van het verzoek om advies.....	3
2.	Beschrijving van de voorontwerpen van wet.....	4
3.	Analyse	6
3.1.	Bevoegdheden en expertisedomeinen van het BIPT.....	6
3.1.1.	<i>Algemeen.....</i>	6
3.1.2.	<i>Bevoegdheden bij de uitvoering van de RTCO.....</i>	7
3.1.3.	<i>Bevoegdheden bij de uitvoering van de DSA</i>	8
3.1.4.	<i>Noodzaak van een aanvullende wettelijke grondslag.....</i>	10
3.1.5.	<i>Keuze van de meest geschikte autoriteit.....</i>	10
3.1.6.	<i>Beroepen tegen de besluiten van het BIPT.....</i>	11
3.2.	Beoogde mechanisme	12
3.2.1.	<i>Aangaande de aanbieders en diensten die in aanmerking kunnen komen</i>	13
3.2.2.	<i>Aangaande de maatregelen die technisch en juridisch het voorwerp kunnen uitmaken van een bevel.....</i>	16
4.	Conclusie	19

1. Voorwerp van het verzoek om advies

1. De minister van Veiligheid en Binnenlandse Zaken heeft op 20 juli 2026 een verzoek om advies gericht aan de voorzitter van het BIPT, met betrekking tot de volgende teksten:

1° een monocameraal voorontwerp van wet *betreffende het administratief verbod op de activiteiten van rechtspersonen, vennootschappen zonder rechtspersoonlijkheid, en feitelijke verenigingen of groeperingen die een ernstige en actuele bedreiging vormen voor de nationale veiligheid*;

2° een bicameraal voorontwerp van wet *betreffende de beroepen bij de Raad van State tegen de administratieve verbodsmaatregelen waarin is voorzien bij de wet van XXX betreffende het administratief verbod op de activiteiten van bepaalde entiteiten die een ernstige en actuele bedreiging vormen voor de nationale veiligheid*.

2. Het advies van het BIPT wordt gevraagd "over de twee voorontwerpen integraal en, in het bijzonder, over de mogelijkheid om te voorzien in een recht voor het BIPT om bevelen uit te vaardigen jegens de dienstenaanbieders teneinde te zorgen voor de daadwerkelijke uitvoering van een verbod om de in het voorontwerp beoogde elektronischecomunicatiemiddelen te gebruiken".

3. Het advies van het BIPT wordt meer bepaald gevraagd voor de volgende punten:

- 1° "de bevoegdheden waarover het BIPT momenteel beschikt";
- 2° "de eventuele noodzaak van een aanvullende wettelijke grondslag";
- 3° "de aanbieders en diensten die in aanmerking kunnen komen";
- 4° "de maatregelen die technisch en juridisch het voorwerp kunnen uitmaken van een bevel";
- 5° "de waarborgen en procedurele regelingen die een dergelijk mechanisme zouden moeten omkaderen".

4. Ten slotte wordt het BIPT gevraagd of de bepalingen die nodig zijn om een dergelijke beveluitvaardigende bevoegdheid in te voeren, volgens het BIPT kunnen worden opgenomen in het voorontwerp van wet dat het wordt voorgelegd of indien deze een specifieke wijziging van de wetgeving met betrekking tot het BIPT vereisen.

5. Bij de opstelling van deze nota heeft het BIPT kennis kunnen nemen van de openbaar beschikbare adviezen, namelijk [advies nr. 2025/9 van 18 september 2025 van het Federaal Instituut voor de bescherming en de bevordering van de Rechten van de Mens](#), [het advies van het College van procureurs-generaal van 25 september 2025](#), [advies 003/VCI/2025 van het Vast Comité I van 9 oktober 2025](#), en [advies 78.110/AG van de Raad van State van 31 december 2025](#).

6. Het BIPT heeft daarentegen geen kennis kunnen nemen van het advies van het CCIV van 8 oktober 2025, waarvan de memorie van toelichting evenwel de inhoud kort samenvat.

7. Rekening houdend met het bestaan van deze eerdere adviezen, en in het kader van zijn bevoegdheden en expertisedomeinen, wijdt het BIPT dit advies aan het onderzoek van de kwesties die in het bijzonder verband houden met de maatregel bedoeld in artikel 5, § 1, 1°, d), die lijkt te kunnen worden gekwalificeerd als maatregel van het type 'digitale verbanning' of maatregel ter beperking van digitale toegang.

2. Beschrijving van de voorontwerpen van wet

8. Het voorontwerp van wet *'betreffende het administratief verbod op de activiteiten van rechtspersonen, vennootschappen zonder rechtspersoonlijkheid, en feitelijke verenigingen of groeperingen die een ernstige en actuele bedreiging vormen voor de nationale veiligheid'* voorziet in administratieve maatregelen die bedoeld zijn om de activiteiten van bepaalde entiteiten te stoppen.
9. Het verbodsmechanisme waarin dit voorontwerp van wet voorziet, stelt de Ministerraad in staat om, op voordracht van de minister van Veiligheid en Binnenlandse Zaken, een administratieve maatregel aan te nemen jegens een van de beoogde entiteiten, met name:
 - rechtspersonen, met uitzondering van de publiekrechtelijke rechtspersonen, bedoeld in artikel 1:5, §§ 2 en 3, artikel 1:6, § 2, en artikel 1:7 van het Wetboek van vennootschappen en verenigingen;
 - vennootschappen zonder rechtspersoonlijkheid, bedoeld in artikel 1:5, § 1, van hetzelfde wetboek;
 - feitelijke verenigingen, bedoeld in artikel 1:6, § 1, van hetzelfde wetboek;
 - feitelijke groeperingen, i.e. groepen natuurlijke personen zonder rechtspersoonlijkheid, die zich op informele wijze organiseren om gezamenlijk een gemeenschappelijk doel na te streven.
10. Een dergelijke entiteit kan een of meer in het voorontwerp van wet vastgelegde verbodsmatregelen opgelegd krijgen *"wanneer uit concrete aanwijzingen blijkt dat zij een ernstige en actuele bedreiging vormt voor de nationale veiligheid, waarbij deze dreiging een essentieel en structureel kenmerk van de betrokken entiteit moet vormen"*. Voor de toepassing van dit voorontwerp van wet wordt verduidelijkt dat *"de nationale veiligheid de bescherming van het voortbestaan van de democratische en grondwettelijke orde, van de democratische instellingen, alsook de bescherming tegen ernstige georganiseerde en systematische inbreuken op de uitoefening van rechten en vrijheden"* omvat (artikel 3, § 3, van het voorontwerp).
11. Het toepassingsgebied van het voorontwerp van wet omvat evenwel niet de representatieve werknemersorganisaties en de politieke partijen die verkiezingskandidaten voordragen gedurende de periode tussen de bekendmaking van de akte waarbij de kiezers worden opgeroepen en de dag van de betrokken stemming (artikel 3, § 1, tweede en derde lid, van het voorontwerp). Er wordt ook gepreciseerd dat de wet *"niet [mag] worden toegepast op de enkele grond dat de betrokken entiteit een politieke, syndicale, religieuze, filosofische of andere opvatting aanhangt, hoe kritisch, controversieel of radicaal deze ook moge zijn"* (artikel 3, § 2, van het voorontwerp) en dat *"De maatregel niet [mag] worden*

gebaseerd op geïsoleerde, incidentele of bijkomstige feiten, noch op gedragingen die toe te schrijven zijn aan bepaalde leden die uitsluitend individueel handelen" (artikel 3, § 4, van het voorontwerp). Wat dat betreft preciseert de memorie van toelichting verder dat *"het administratief verbod geen veroordeling [is], maar een bijzondere politiemaatregel die gericht is tegen de structuur en niet tegen de personen die daarvan deel uitmaken."*

12. Naar aanleiding van het advies van de Raad van State lijst artikel 4 de drie cumulatieve voorwaarden op waaraan moet voldaan zijn om een administratieve verbodsmaatregel te kunnen aannemen, met name: 1° de vaststelling van feiten die van die aard zijn dat ze aantonen dat de entiteit een ernstige en actuele bedreiging vormt in de zin van artikel 3 (opgesomd in artikel 4, eerste lid, 1°); 2° het bestaan van een concreet verband met het Belgische grondgebied; 3° de noodzakelijkheid en evenredigheid van de beoogde maatregelen.
13. Onder de administratieve maatregelen die kunnen worden aangenomen, valt ook het verbod om digitale tools aan te wenden om de werking van de betrokken entiteit te organiseren, te bevorderen, te coördineren, te ondersteunen of voort te zetten.
14. Artikel 5, § 1, 1°, d), van het voorontwerp van wet bepaalt immers dat:

*"§ 1. Naargelang de juridische aard van de betrokken entiteit, de ernst van de vastgestelde dreiging en het evenredigheidsbeginsel, kan het verbod bestaan uit:
1° één of meerdere administratieve maatregelen bestaande uit alle of een deel van de volgende maatregelen: (...)
d) het verbod om digitale platforms, websites, accounts op sociale media, berichtkanalen of andere digitale communicatiemiddelen te gebruiken, die hoofdzakelijk of op doorslaggevende wijze worden aangewend om de werking van de betrokken entiteit te organiseren, te bevorderen, te coördineren, te ondersteunen of voort te zetten; (...)"*
15. Artikel 8, § 1, eerste lid, bepaalt dat: *"§ 1. De in artikel 5, § 1, 1° bedoelde maatregelen worden aangenomen bij koninklijk besluit, genomen na beraadslaging in de ministerraad, op voorstel van de minister."*
16. Artikel 5, § 3, eerste lid, geeft per categorie van administratieve maatregelen aan welke autoriteit bevoegd is voor de uitvoering ervan. In tegenstelling tot voor de andere types van maatregelen wordt voor de voormelde categorie d) (i.e. het verbod op het gebruik van bepaalde digitale-communicatiemiddelen), geen enkele uitvoerende verantwoordelijkheid vermeld.
17. Het voorontwerp van wet 'betreffende de beroepen bij de Raad van State tegen de administratieve verbodsmaatregelen waarin is voorzien bij de wet van XXX betreffende het administratief verbod op de activiteiten van bepaalde entiteiten die een ernstige en actuele bedreiging vormen voor de nationale veiligheid' regelt een specifiek rechtsmiddel tegen de administratieve maatregelen die worden aangenomen in uitvoering van dit ontwerp.

3. Analyse

18. Overeenkomstig het verzoek geformuleerd door mijnheer de Minister van Veiligheid en Binnenlandse Zaken, volgt hieronder een tweeledig antwoord:
- 18.1. *Een eerste deel* betreft de bevoegdheden en expertisedomeinen van het BIPT (punt 3.1 hieronder);
- 18.2. *Een tweede deel* handelt over het beoogde mechanisme en in het bijzonder over de administratieve maatregel ter beperking van digitale toegang, bedoeld in artikel 5, § 1, 1^o, d), van het eerste voorontwerp van wet (punt 3.2 hierna).

3.1. Bevoegdheden en expertisedomeinen van het BIPT

3.1.1. Algemeen

19. Het BIPT is een instelling van openbaar nut met rechtspersoonlijkheid, waarvan de opdrachten hoofdzakelijk zijn opgelijst in artikel 14 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, hierna 'de wet betreffende het statuut van het BIPT'. Die wet werd de voorbije jaren aangevuld om het BIPT met name bijzondere opdrachten toe te vertrouwen met betrekking tot bepaalde aanbieders van diensten van het digitale ecosysteem.
20. Het gaat meer bepaald over controle- en sanctiebevoegdheden in het kader van de strijd tegen de verspreiding van terroristische online-inhoud in de zin van de Verordening (EU) 2021/784 van het Europees Parlement en Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, hierna de 'RTCO' (zie punt 3.1.2. hieronder), van toepassing op de aanbieders van 'hostingdiensten'¹. Daarnaast werd het BIPT ook belast met de tenuitvoerlegging op federaal niveau, het toezicht en de sancties in geval van niet-naleving van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaaldienstenverordening), hierna 'DSA' voor 'Digital Services Act' (zie punt 3.2.1 hieronder), van toepassing op de aanbieders van 'tussenhandeldiensten'².
21. Het BIPT is ook de federale instantie die optreedt als regulator in de mediasector in het tweetalige gebied Brussel-Hoofdstad wat betreft de audiovisuele mediadiensten en de videoplatformdiensten die noch onder de bevoegdheid van de Vlaamse Gemeenschap noch onder deze van de Franse Gemeenschap vallen (wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad).

¹ In de zin van artikel 2, eerste lid, 1), van de RTCO.

² In de zin van artikel 3, eerste lid, g), van de DSA.

22. Zijn specifieke sectorale bevoegdheden zijn vastgelegd in andere specifieke wetten³, hoofdzakelijk de wet van 13 juni 2005 betreffende de elektronische communicatie, hierna 'WEC', wat betreft radiospectrumbeheer, elektronischecommunicatieregulering, nummering, bescherming van de maatschappij en de gebruikers, beveiliging van de elektronische communicatie, bescherming van de eindgebruikers enz.

3.1.2. Bevoegdheden bij de uitvoering van de RTCO

23. De RTCO heeft tot doel gemeenschappelijke regels vast te stellen om ervoor te zorgen dat aanbieders van hostingdiensten het misbruik van hun diensten voor het verspreiden van terroristische inhoud tegengaan en de openbare veiligheid beschermen, waarbij tegelijk de eerbiediging van de grondrechten, met name de vrijheid van meningsuiting en de vrijheid van informatie, wordt gewaarborgd.
24. In het kader van de RTCO is het BIPT de bevoegde autoriteit voor de specifieke opdrachten opgelijst in artikel 12, lid 1, c) en d) van de RTCO, onverminderd de taken die zijn toevertrouwd aan de federale procureur krachtens artikel 12, lid 1, a) en b), van de RTCO.⁴ De opdrachten van het BIPT hebben dan ook betrekking op het toezicht op de uitvoering van de specifieke maatregelen op grond van artikel 5 van de RTCO⁵ en het opleggen van sancties op grond van artikel 18 van de RTCO⁶. Die laatste opdracht omhelst met name de mogelijkheid om sancties op te leggen voor de niet-naleving van bevelen tot verwijdering van terroristische inhoud of bevelen tot het blokkeren van toegang tot die inhoud in het geheel van de lidstaten, uitgevaardigd door de bevoegde autoriteiten van de lidstaten. Het BIPT is echter niet bevoegd om zelf dergelijke bevelen tot verwijdering of blokkering van inhoud uit te vaardigen. In België is de federale procureur hiervoor bevoegd⁷ en zorgt de federale politie voor de praktische uitvoering ervan.
25. De aanbieders op wie de RTCO van toepassing is, zijn de 'aanbieders van hostingdiensten', zoals gedefinieerd in artikel 2, lid 1, punt 1, van de RTCO,⁸ voor zover ze informatie verspreiden onder het publiek.⁹
26. De RTCO berust op het principe van toezicht door de lidstaat waar de dienstaanbieder is gevestigd. Conform artikel 16 van de RTCO is de lidstaat waarin de aanbieder van hostingdiensten zijn hoofdzetel heeft, of waarin zijn wettelijke vertegenwoordiger verblijft of gevestigd is, bevoegd voor het toezicht op de tenuitvoerlegging van de specifieke maatregelen waarin artikel 5 van de RTCO voorziet, alsook om sancties op te leggen

³ We vestigen uiteraard de aandacht op de wet van 26 januari 2018 betreffende de postdiensten, maar ook op de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: het BIPT oefent de functie uit van sectoroverheid en van inspectiedienst voor de digitale infrastructuur (met uitzondering van de vertrouwensdienstverleners) en voor de sector van de post- en koerierdiensten. Ten slotte merken we op dat het BIPT krachtens de wet van 19 december 2025 betreffende de weerbaarheid van kritieke entiteiten, de sectoroverheid is die toezicht houdt op de kritieke infrastructuur in de sector van de digitale infrastructuur (met uitzondering van de vertrouwensdienstverleners).

⁴ Artikel 14, § 1, 3^o, l), van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, *BS*, 24 januari 2003.

⁵ Artikel 12, lid 1, c), van de RTCO.

⁶ Artikel 12, lid 1, d), van de RTCO.

⁷ Artikel 144bis, § 2, eerste lid, 4^o, van het Gerechtelijk Wetboek, conform de richtsnoeren vastgelegd in een omzendbrief van het College van procureurs-generaal en artikel 12, lid 1, a), van de RTCO.

⁸ Zie punt 3.2.1 infra.

⁹ Artikel 1, lid 2, van de RTCO.

conform artikel 18 van de RTCO. Het BIPT is bijgevolg enkel bevoegd voor de uitoefening van die opdrachten jegens de aanbieders van hostingdiensten met hoofdzetel in België of die hun wettelijke vertegenwoordiger in de zin van de RTCO in België hebben aangewezen.

3.1.3. Bevoegdheden bij de uitvoering van de DSA

27. De DSA beoogt te zorgen voor een veiligere en eerlijkere onlineomgeving voor gebruikers door de aanbieders van onlinetussenhandeldiensten bepaalde zorgvuldigheidsverplichtingen op te leggen, zoals transparantie in geval van verwijdering van inhoud, de mogelijkheid om gemakkelijk illegale inhoud te melden enz.
28. In het kader van de tenuitvoerlegging van de DSA, werd het BIPT aangewezen als enerzijds de nationale digitaledienstencoördinator (hierna 'DSC') in het kader van het samenwerkingsakkoord van 3 mei 2024¹⁰ en anderzijds als bevoegde autoriteit op federaal niveau¹¹. Verder werden ook de Conseil supérieur de l'audiovisuel (CSA), de Medienrat en de Vlaamse Regulator voor de Media (VRM) aangewezen als autoriteiten die bevoegd zijn voor de tenuitvoerlegging van de DSA in België, binnen de bevoegdheden die zijn toegekend aan de gemeenschappen.
29. Het samenwerkingsakkoord van 3 mei 2024 regelt de gecoördineerde tenuitvoerlegging van de DSA in België. Het bepaalt principieel dat de bevoegde autoriteiten en de DSC de DSA uitvoeren in overeenstemming met hun respectievelijke bevoegdheden.¹² In zijn hoedanigheid van DSC is het BIPT verantwoordelijk voor de coördinatie op nationaal niveau voor alle kwesties die verband houden met het toezicht op en de handhaving van de DSA en draagt het bij aan het effectieve en consistente toezicht op en de handhaving van de DSA in de hele EU.¹³ De volledige lijst van de opdrachten van de DSC staat beschreven in artikel 2, § 2, tweede lid, van het samenwerkingsakkoord. Tot de opdrachten behoren met name de centralisering van de bevelen afkomstig van de Belgische sectorale autoriteiten zoals bedoeld in de artikelen 9 en 10 van de DSA.
30. Wat betreft de verplichtingen zoals vastgelegd in de artikelen 9 en 10 van de DSA, is de aangewezen bevoegde autoriteit¹⁴ niet belast met het toezicht op of de tenuitvoerlegging van het bevel om inhoud te verwijderen of informatie te verstrekken over een of meer gebruikers van de dienst, gericht aan de aanbieder van tussenhandeldiensten. Die bevoegdheid behoort toe aan de sectorale administratieve of gerechtelijke autoriteit die het bevel heeft uitgevaardigd op grond van het toepasselijke recht.
31. De bevoegde autoriteit in de zin van de DSA heeft echter tot taak na te gaan of de betrokken aanbieder van tussenhandeldiensten de procedurele verplichtingen heeft nageleefd die artikel 9 van de DSA hem oplegt als gevolg van een bevel, zoals de informatie- en follow-upverplichtingen. In België zal welke autoriteit bevoegd is om in een

¹⁰ Artikel 14, § 1, van het samenwerkingsakkoord van 3 mei 2024 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap en de Duitstalige Gemeenschap met betrekking tot de gecoördineerde tenuitvoerlegging van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening), *BS*, 30 december 2024.

¹¹ Artikel 14, § 1/1, van de voormelde wet van 17 januari 2003 (statuut): "*Wat de federale bevoegdheden betreft, is het Instituut een bevoegde autoriteit in de zin van artikel 49 van de digitaledienstenverordening.*"

¹² Artikel 3 en 4, § 2, derde lid, van het samenwerkingsakkoord van 3 mei 2024.

¹³ Artikel 4, § 2, eerste lid, van het samenwerkingsakkoord van 3 mei 2024.

¹⁴ Bevoegde autoriteit in de zin van: autoriteit bevoegd voor de tenuitvoerlegging van de DSA.

specifiek geval toezicht te houden op de naleving van deze verplichtingen uiteindelijk afhangen van het bestuursniveau dat bevoegd is voor de betreffende aangelegenheid.

32. Algemeen moet worden opgemerkt dat de DSA het begrip 'illegale inhoud' definieert door te verwijzen naar het toepasselijke materiële recht, zonder zelf regels vast te stellen die bepalen welke inhoud illegaal is.¹⁵ Het is niet de taak van de bevoegde autoriteiten die belast zijn met het toezicht op en de handhaving van de DSA om, bij de uitoefening van de bevoegdheden die hun in het kader daarvan zijn toegekend, algemeen toezicht te houden op inhoud die online verspreid wordt, met het oog op het opsporen of aanmerken van individuele inhoudselementen als illegaal. Hun taak bestaat er in de eerste plaats in te controleren of de aanbieders van tussenhandeldiensten de verplichtingen naleven die de DSA hen oplegt en die voornamelijk uit zorgvuldigheidsverplichtingen bestaan. Zo voorziet artikel 28 van de DSA (over de 'bescherming van minderjarigen') bijvoorbeeld verplichtingen in verband met risicobeheer die veeleer kunnen worden beschouwd als middelenverbintenissen die erop gericht zijn geïdentificeerde risico's te beperken.¹⁶
33. Teneinde te onderzoeken of aan deze verplichtingen is voldaan, zal de bevoegde autoriteit hoofdzakelijk de maatregelen, processen en mechanismen bekijken die zijn ingevoerd door de aanbieder, zoals, met name in het kader van artikel 28 van de DSA, eventuele beperkingen van de toegang tot de dienst, de standaardinstellingen, het online-interfaceontwerp, aanbevelingssystemen en zoekfuncties of inhoudsmoderatiesystemen om zo een hoog niveau van privacy, veiligheid en bescherming van minderjarigen binnen hun dienst te waarborgen. De controle is dus niet in hoofdzaak op de inhoud gericht. Ze is daarentegen gericht op de reactie van de aanbieder op het betreffende risico, en niet op de juridische kwalificatie van afzonderlijk genomen individuele inhoud als dusdanig.¹⁷
34. De aanbieders op wie de DSA van toepassing is, zijn de aanbieders van 'tussenhandeldiensten', zoals gedefinieerd in artikel 3, lid 1, punt g) van de DSA.¹⁸ In overeenstemming met artikel 56 van de DSA wordt de bevoegdheid jegens een aanbieder van tussenhandeldiensten bepaald door de lidstaat waarin deze zijn hoofdzetel heeft¹⁹ of waarin zijn wettelijke vertegenwoordiger verblijft of is gevestigd. Die lidstaat heeft de exclusieve bevoegdheid om toezicht te houden op de DSA de verordening te doen naleven, onverminderd de bevoegdheden die aan de Europese Commissie zijn verleend met betrekking tot zeer grote onlineplatforms en zeer grote onlinezoekmachines.
35. Daaruit vloeit voort dat enkel de aanbieders van tussenhandeldiensten die hun hoofdzetel in België hebben, evenals zij die een wettelijke vertegenwoordiger hebben aangewezen in België, onder de bevoegdheid vallen van de Belgische autoriteiten die bevoegd zijn voor

¹⁵ Artikel 3, eerste lid, h), van de DSA.

¹⁶ Artikel 28 van de DSA bepaalt dat de aanbieders van voor minderjarigen toegankelijke onlineplatforms passende en evenredige maatregelen moeten nemen om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen binnen hun dienst te waarborgen. De richtsnoeren van de Europese Commissie die zijn aangenomen overeenkomstig artikel 28, lid 4, formuleren wat dat betreft aanbevelingen voor de betreffende aanbieders van onlineplatforms.

¹⁷ Het aantal gemelde inhoudselementen dat als schadelijk voor de privacy, veiligheid en bescherming van minderjarigen wordt beschouwd, kan evenwel bijkomstig in aanmerking worden genomen, voor zover dat nodig is om de geschiktheid, evenredigheid en doeltreffendheid van de door de aanbieder genomen maatregelen te beoordelen.

¹⁸ Zie punt 3.3 infra.

¹⁹ Met andere woorden, overeenkomstig overweging 123 van de DSA: de lidstaat "waar de aanbieder zijn hoofdkantoor of wettelijke zetel heeft en waar de belangrijkste financiële functies en operationele controle worden uitgeoefend".

de tenuitvoerlegging van de DSA, waaronder het BIPT. Het toezicht op de verplichtingen die door de DSA zijn vastgesteld ten aanzien van de aanbieders van tussenhandeldiensten die niet onder de Belgische bevoegdheid vallen, wordt uitgeoefend door de bevoegde DSC in kwestie en, in voorkomend geval, de Europese Commissie.

3.1.4. Noodzaak van een aanvullende wettelijke grondslag

36. Tot op heden beschikt het BIPT niet over de nodige wettelijke grondslagen om op te treden in het kader van de tenuitvoerlegging van maatregelen ter beperking van digitale toegang, zoals beoogd in het eerste voorontwerp van wet dat ter advies werd voorgelegd.
37. In het geval dat een uitbreiding van de bevoegdheden van het BIPT zou moeten worden overwogen, is het van belang erop te wijzen dat zijn wettelijke opdrachten, op zijn minst in beginsel, opgesomd zijn in artikel 14 van de bovengenoemde wet betreffende het statuut van het BIPT.
38. In tegenstelling tot voor de andere maatregelen beoogd in het eerste voorontwerp van wet, wordt voor de in artikel 5, § 1, 1°, d) van het ontwerp beoogde categorie (i.e. het verbod op het gebruik van bepaalde digitale-communicatiemiddelen), geen enkele uitvoerende verantwoordelijkheid vermeld. Doordat dit niet wordt gepreciseerd, zou het, zoals de teksten momenteel zijn opgesteld, aan de Koning zijn om de autoriteit aan te wijzen die verantwoordelijk is voor de uitvoering van de maatregel bedoeld in d). Dat bemoeilijkt elke deelname van het BIPT op juridisch vlak aangezien enkel de wetgever nieuwe opdrachten kan toewijzen aan een onafhankelijke administratieve overheid zoals het BIPT.

3.1.5. Keuze van de meest geschikte autoriteit

39. Alvorens een eventuele aanvullende wettelijke grondslag te beogen die het BIPT een nieuwe bevoegdheid toevertrouwt in het kader van het beoogde mechanisme, rijst de vraag of het BIPT de meest geschikte autoriteit is om de opdracht van toezicht op de goede uitvoering van de beoogde maatregelen ter beperking van digitale toegang op zich te nemen. Dat lijkt echter niet het geval, om de hierna uiteengezette redenen.
40. In uitvoering van de RTCO is het BIPT verantwoordelijk voor administratieve sancties op de niet-naleving van de bevelen tot verwijdering of blokkering van terroristische inhoud die zijn uitgevaardigd door de federale procureur of door de bevoegde autoriteiten van andere lidstaten, zodra deze definitief zijn geworden. Daarbij kan het BIPT, in geval van inbreuk en overeenkomstig artikel 21 van de wet betreffende het statuut van het BIPT, de aanbieder van hostingdiensten bevelen een einde te maken aan de inbreuk, in voorkomend geval aan de hand van een dwangsom en/of deze veroordelen tot een administratieve boete.
41. Niettemin heeft het BIPT bij de uitoefening van deze opdracht geenszins beoordelingsvrijheid ten aanzien van de inhoud van het bevel als zodanig en wordt het niet geacht de noodzaak of evenredigheid van dit bevel te beoordelen. Die opdrachten zijn in de eerste plaats voorbehouden aan de beveluitvaardigende autoriteit en eventueel, in de tweede plaats, aan de beroepsinstanties en -autoriteiten die verantwoordelijk zijn voor een grondig onderzoek van het in artikel 4, lid 3, van de RTCO bedoelde grensoverschrijdende verwijderingsbevel. Deze laatste procedure heeft tot doel vast te stellen of het

verwijderingsbevel ernstig of kennelijk in strijd is met de RTCO of met de door het Handvest gewaarborgde grondrechten en vrijheden, en valt in België onder de bevoegdheid van de federale procureur.²⁰

42. In het kader van de DSA is de bevoegdheid van het BIPT eveneens in principe beperkt tot het verifiëren van de procedurele verplichtingen die aan dienstaanbieders worden opgelegd in het kader van bevelen om tegen illegale inhoud op te treden.
43. De administratieve sanctieprocedure waarmee het BIPT is belast, biedt uiteraard aanzienlijke voordelen op het vlak van efficiëntie. De aard van deze administratieve sanctiebevoegdheid verschilt echter sterk van de aard van de bevoegdheid om bevelen uit te vaardigen. De uitoefening van een dergelijke bevoegdheid, veronderstelt immers expertise inzake de opsporing van illegale inhoud en de juridische kwalificatie van deze inhoud, waarover het BIPT niet beschikt.
44. Hoe kan immers de doeltreffendheid van een maatregel ter beperking van de digitale toegang van een bepaalde entiteit gecontroleerd worden, anders dan door na te gaan of deze entiteit niet opnieuw opduikt via een nieuw gebruikersaccount, en dus door inhoud op te sporen die verband houdt met de activiteiten van deze entiteit?
45. In het kader van terroristische inhoud, staat in de praktijk de Federal Computer Crime Unit (FCCU) – Internet Referral Unit (IRU) van de federale politie in voor de opsporing van de inhoud. Binnen tal van andere domeinen zijn het de federale overheidsdiensten die illegale online-inhoud opsporen. Dat is bijvoorbeeld het geval voor de Dienst voor de Strijd tegen Inbreuken op het Auteursrecht en de Naburige Rechten op het Internet en tegen de exploitatie van onwettige onlinekansspelen. Die dienst is bij koninklijk besluit van 18 april 2024 opgericht binnen de Algemene Directie Economische Inspectie van de FOD Economie.²¹ In voorkomend geval zou dan ook kunnen overwogen worden om een gespecialiseerde inspectiedienst in het leven te roepen binnen de FOD Binnenlandse Zaken, de FOD Justitie of de FOD Kanselarij van de Eerste Minister.²²

3.1.6. Beroepen tegen de besluiten van het BIPT

46. Tot slot is het, op vlak van beroepsmogelijkheden, nuttig te preciseren dat de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (hierna 'de rechtsmiddelenwet') het Marktenhof, dat in kort geding uitspraak doet, de opdracht toevertrouwt uitspraak te doen over een beroep met volle rechtsmacht tegen de besluiten van het BIPT betreffende de aanbieders die onder de bevoegdheid van het BIPT vallen. Wanneer het beroep gericht is tegen een besluit van reglementaire aard, beschikt het Marktenhof enkel over een vernietigingsrecht.

²⁰ Artikel 144bis, § 2, eerste lid, 4°, van het Gerechtelijk Wetboek, conform de richtsnoeren vastgelegd in een omzendbrief van het College van procureurs-generaal en artikel 12, lid 1, b), van de RTCO.

²¹ Zie de webpagina van de Dienst, <https://economie.fgov.be/nl/themas/intellectuele-eigendom/intellectuele-eigendomsrechten/auteursrecht-en-naburige/sancties-en-gerechtelijke/online-piraterij>.

²² Zie met name het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *BS*, 21/11/2014.

47. Gezien de regeling voor beroepen tegen besluiten van het BIPT bij het Marktenhof, zou de organisatie van een specifieke beroepsprocedure bij de Raad van State dan ook een aanpassing van de eerdergenoemde 'rechtsmiddelenwet' van 17 januari 2003 vereisen, wat zou kunnen leiden tot een systeem dat voor de actoren in de digitale sector moeilijk te begrijpen is.

3.2. Beoogde mechanisme

48. De vragen gesteld door mijnheer de Minister van Veiligheid en Binnenlandse Zaken werpen onvermijdelijk de onderliggende kwestie op van de juridische en praktische haalbaarheid van de beoogde administratieve maatregel.
49. In dit kader dient er eerst op te worden gewezen dat artikel 5, § 1, 1^o, d) van het voorontwerp²³ beoogt een administratieve maatregel van zeer algemene strekking in te voeren, bestaande in *"het verbod om digitale platforms, websites, accounts op sociale media, berichtkanalen of andere digitale communicatiemiddelen te gebruiken, die hoofdzakelijk of op doorslaggevende wijze worden aangewend om de werking van de betrokken entiteit te organiseren, te bevorderen, te coördineren, te ondersteunen of voort te zetten"*.
50. Artikel 5, § 3, eerste lid, van het wetsontwerp geeft per categorie van administratieve maatregelen aan welke overheid bevoegd is voor de uitvoering ervan. Het BIPT merkt evenwel op dat voor categorie d) (i.e. het verbod op het gebruik van bepaalde digitale-communicatiemiddelen), geen enkele uitvoerende verantwoordelijkheid wordt vermeld.
51. Toegegeven, het tweede lid van dezelfde paragraaf bepaalt dat het in artikel 8 bedoelde koninklijk besluit voor elke aangenomen maatregel de autoriteiten en diensten aanwijst die verantwoordelijk zijn voor de uitvoering en de controle ervan. Het derde lid voegt hieraan toe: *"De aldus aangewezen overheden en diensten stellen de materiële, administratieve of technische handelingen die strikt noodzakelijk zijn voor de daadwerkelijke uitvoering van de maatregelen die hen betreffen"* (Wij onderlijnen). Volgens het vierde lid *"kunnen [zij] daartoe aan de rechtstreeks betrokken personen, instellingen of dienstverleners de bevelen richten die strikt noodzakelijk zijn voor die uitvoering, voor zover die bevelen rechtstreeks verband houden met de bij het koninklijk besluit genomen maatregelen, beperkt blijven tot de daadwerkelijke uitvoering ervan en evenredig zijn aan de vastgestelde dreiging."* (Wij onderlijnen). Ten slotte luidt het vijfde lid: *"Deze bevelen mogen de draagwijdte van de bij het koninklijk besluit genomen maatregelen niet wijzigen, noch nieuwe verboden invoeren."*
52. De tenuitvoerbrenging van het beoogde mechanisme berust dus op **verscheidene besluitvormingsniveaus**.

²³ "Art. 5. § 1. Naargelang de juridische aard van de betrokken entiteit, de ernst van de vastgestelde dreiging en het evenredigheidsbeginsel, kan het verbod bestaan uit:

1^o één of meerdere administratieve maatregelen bestaande uit alle of een deel van de volgende maatregelen: [...]

d) het verbod om digitale platforms, websites, accounts op sociale media, berichtkanalen of andere digitale communicatiemiddelen te gebruiken, die hoofdzakelijk of op doorslaggevende wijze worden aangewend om de werking van de betrokken entiteit te organiseren, te bevorderen, te coördineren, te ondersteunen of voort te zetten; [...]"

- 52.1. Een na overleg in de Ministerraad vastgesteld koninklijk besluit bepaalt:
 - i. de entiteit waarop de verbodsmaatregel van toepassing is;
 - ii. het soort van maatregel (in dit geval de beperking van digitale toegang waarin artikel 5, § 1, 1^o, d) voorziet), en;
 - iii. de uitvoerende autoriteit/dienst;
- 52.2. Een bevel uitgevaardigd door een administratieve overheid bepaalt:
 - i. De te nemen concrete maatregelen, voor zover zij beperkt zijn tot "*de daadwerkelijke uitvoering*" van het verbod en "*evenredig zijn aan de vastgestelde dreiging*";
 - ii. De ontvangende "*rechtstreeks betrokken personen, instellingen of dienstverleners*" die worden opgedragen deze maatregelen te nemen;
- 52.3. Een controle van de uitvoering van deze maatregelen door de(zelfde?) administratieve autoriteit;
- 52.4. Een daadwerkelijke beroepsmogelijkheid tegen elk van deze administratieve besluiten.

3.2.1. Aangaande de aanbieders en diensten die in aanmerking kunnen komen

53. Een ***eerste juridische moeilijkheid*** die zich voordoet bij de bepaling van welke aanbieders en diensten in aanmerking kunnen komen, betreft de **soorten beoogde diensten**; de begrippen zijn niet gedefinieerd in het voorontwerp en stemmen niet overeen met begrippen die zijn vastgelegd in Belgisch of Europees recht. Ter wille van de rechtszekerheid, maar ook met het oog op de evenredigheid, is het echter van belang de betrokken diensten duidelijk te omschrijven. Zoals de tekst er nu uitziet, lijken deze doelstellingen niet vervuld.
54. Zo is het bijvoorbeeld niet duidelijk of de betreffende diensten enkel de 'openbare' communicatiekanalen beogen of ook de 'private'²⁴. Het is evenmin duidelijk of dit de

²⁴ In dit verband merken we op dat zowel de DSA als de RTCO rekening houden met de manier waarop de toegang tot informatie wordt verkregen, met name in een groep of een kanaal. Er wordt namelijk bekeken of er toegangsbeperkingen bestaan en of er automatisch toestemming wordt gegeven of pas na een menselijke handeling. Overweging 14 van de DSA geeft aan: "*Het begrip "verspreiding onder het publiek", [...] moet inhouden dat informatie beschikbaar wordt gesteld aan een potentieel onbeperkt aantal personen, dat wil zeggen dat de informatie gemakkelijk toegankelijk wordt gemaakt voor afnemers van de dienst in het algemeen zonder dat de informatieverstrekken afnemer van de dienst daar verder iets voor hoeft te doen, ongeacht of die personen de betrokken informatie daadwerkelijk raadplegen. Indien voor de toegang tot informatie registratie of toelating tot een groep afnemers van de dienst vereist is, mag die informatie dan ook alleen worden geacht onder het publiek te zijn verspreid wanneer afnemers van de dienst die toegang tot de informatie wensen automatisch worden geregistreerd of toegelaten zonder menselijke beslissing of selectie van wie toegang krijgt.*" en zie ook overweging 14 van de RTCO.

nummergebaseerde en nummeronafhankelijke interpersoonlijke communicatiediensten omvat. Een ruime interpretatie van "*berichtkanalen of andere digitale communicatiemiddelen*" zou er *a priori* toe kunnen leiden dat private communicatie (bijvoorbeeld spraakoproepen en sms'en) in de werkingssfeer van de bepaling wordt opgenomen.

55. Om de beoogde diensten beter te definiëren en de algemene samenhang tussen de normen te waarborgen, zou zoveel mogelijk gebruik moeten worden gemaakt van de begrippen die op Europees niveau zijn gedefinieerd, hetzij in het Europees wetboek voor elektronische communicatie (hierna 'het Wetboek'), de DSA, de RTCO of Verordening 2022/1925 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitaalemarktenverordening) of DMA voor 'Digital Markets Act'.

56. Zo zou een analyse van de volgende Europese begrippen – die hieronder op niet-uitputtende wijze worden weergegeven – reeds kunnen bijdragen tot een nauwkeurigere afstemming van de reikwijdte van de maatregel op de nagestreefde doelstelling:

1° "**interpersoonlijke communicatiedienst**", gedefinieerd als "*een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronische-communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;*" (art. 2, lid 1, punt 5, van het Wetboek). Uit de memorie van toelichting blijkt *a priori* niet dat het de bedoeling zou zijn om dergelijke communicatie van private aard te beogen. Dat type communicatie is beschermd door de geheimhouding van private elektronische communicatie (artikel 5 van Richtlijn 2002/58/EG²⁵). Dat punt verdient verdere verduidelijking.

2° "**tussenhandeldienst**": in het kader van de DSA wordt deze notie gebouwd op de notie van "dienst van de informatiemaatschappij", "*een "dienst" in de zin van artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535,*" en die bestaat in een "mere conduit-dienst", een "caching-dienst" of een "hosting-dienst" (artikel 3, eerste lid, punt a) en g) van de DSA).

3° "**hostingdienst**": in het kader van de DSA wordt deze gedefinieerd als een tussenhandeldienst, namelijk een dienst van de informatiemaatschappij bestaande "*in de opslag van de door een afnemer van de dienst verstrekte informatie*" (artikel 3, eerste lid, punt g), iii), van de DSA). In het kader van de RTCO wordt een "aanbieder van hostingdiensten" gedefinieerd als "*een aanbieder van diensten als gedefinieerd in artikel 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (14) die erin bestaan informatie die door een aanbieder van inhoud is verstrekt, op diens verzoek op te slaan,*" (artikel 2, eerste lid, punt 1, van de RTCO). De definities van hostingdienst in de DSA en in de RTCO verwijzen aldus beide naar het begrip 'dienst van de informatiemaatschappij' evenals naar het technische kenmerk van het opslaan van

²⁵ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), *PBL 201* van 31/07/2002, blz. 0037 - 0047.

informatie die door een gebruiker op diens verzoek wordt verstrekt²⁶. De RTCO beperkt zijn toepassingsgebied echter tot aanbieders van hostingdiensten “voor zover zij informatie onder het publiek verspreiden”²⁷, zodat het toepassingsgebied in de praktijk dichter bij het begrip “onlineplatform” in de zin van de DSA ligt, zoals hieronder beschreven.

4° “**onlineplatform**”, is een subcategorie van hostingdiensten, gedefinieerd als “een hostingdienst die, op verzoek van een afnemer van de dienst, informatie opslaat en verspreidt bij het publiek, tenzij die activiteit een klein of een louter bijkomend kenmerk van een andere dienst of een kleine functionaliteit van de hoofddienst uitmaakt en om objectieve en technische redenen niet kan worden gebruikt zonder die andere dienst, en de integratie van het kenmerk of de functionaliteit in de andere dienst geen manier is om de toepasbaarheid van deze verordening te omzeilen” (artikel 3, eerste lid, punt i) van de DSA).²⁸

5° “**sociale media**”: De DSA biedt geen op zich staande definitie van socialenetwerkdiensten. Deze diensten kunnen echter binnen de categorie van onlineplatforms in de zin van artikel 3, eerste lid, punt i), van de DSA vallen, mits zij voldoen aan de samenstellende elementen van die definitie. Ter indicatie kan worden opgemerkt dat artikel 2, lid 1, punt 7, van de DMA een “**onlinesocialenetwerkdienst**” definieert als “een platform dat eindgebruikers in staat stelt via meerdere apparaten met elkaar in verbinding te treden en te communiceren, inhoud te delen en andere gebruikers en inhoud te ontdekken, met name via chats, posts, video’s en aanbevelingen”. In deze definitie wordt echter niet aangegeven wat de reikwijdte is van het begrip “andere gebruikers en inhoud te ontdekken”. De definitie wordt slechts ter referentie vermeld, aangezien het BIPT geen bijzondere bevoegdheid heeft voor de toepassing van of het toezicht op de DMA.

57. Aangezien de grenzen tussen socialenetwerkdiensten en andere categorieën digitale diensten vervagen, bestaat het risico dat een te enge of te specifieke definitie de snelle ontwikkeling van digitale diensten niet langer voldoende weerspiegelt en dat ze snel achterhaald raakt. Omgekeerd berust de DSA op ruim gedefinieerde categorieën, zoals het “**onlineplatform**”, dat in de praktijk verscheidene diensten kan omvatten die algemeen als sociale netwerken worden beschouwd, maar ook andere diensten die gebruikers in staat stellen informatie te verspreiden onder het publiek kan omvatten.
58. Ten slotte zij erop gewezen dat de **traditionele websites**, die geen door derden verstrekte informatie opslaan, niet onder de definitie van tussenhandeldiensten of hostingdiensten vallen. Zij zijn zelf verantwoordelijk voor hun eigen inhoud.
59. Een **tweede juridische moeilijkheid** schuilt in de beperking van het verbod van het gebruik van diensten “die hoofdzakelijk of op doorslaggevende wijze worden aangewend

²⁶ In het kader van de DSA “afnemer” en in het kader van de RTCO “aanbieder van inhoud”.

²⁷ Artikel 1, lid 2, van de RTCO.

²⁸ We wijzen erop dat overweging 14 van de DSA stelt dat: “**Interpersoonlijke communicatiediensten, zoals gedefinieerd in Richtlijn (EU) 2018/172 van het Europees Parlement en de Raad, zoals e-mails of particuliere berichtendiensten, vallen niet onder de definitie van onlineplatforms, aangezien zij worden gebruikt voor interpersoonlijke communicatie tussen een door de afzender van de communicatie bepaald eindig aantal personen. De in deze verordening uiteengezette verplichtingen voor aanbieders van onlineplatforms kunnen echter van toepassing zijn op diensten waarmee informatie ter beschikking kan worden gesteld van een mogelijk onbeperkt aantal afnemers dat niet door de afzender van de communicatie wordt bepaald, zoals via openbare groepen of vrij toegankelijke kanalen. Informatie mag alleen worden beschouwd als verspreid onder het publiek in de zin van deze verordening wanneer die verspreiding gebeurt op rechtstreeks verzoek van de informatieverstrekende afnemer van de dienst.**”

om de werking van de betrokken entiteit te organiseren, te bevorderen, te coördineren, te ondersteunen of voort te zetten".

60. Het BIPT veronderstelt dat het doel van de maatregel is om een verbod op te leggen op het gebruik van een specifieke dienst waarvoor is vastgesteld dat deze voor de bovengenoemde doeleinden wordt gebruikt. Een verbod op het gebruik van alle diensten door voortdurende controle op de onlineactiviteiten van de betrokken entiteit zou moeilijker te rechtvaardigen zijn in termen van evenredigheid en grondrechten. Ook de kwestie van de doeleinden van het gebruik dient zich aan: is de beperking van toegang tot bepaalde communicatiemiddelen van toepassing zonder uitzonderingen of is ze enkel bedoeld voor de strafbare handelingen van de entiteit die de maatregel opgelegd krijgt? In dat laatste geval zou de controle van de uitvoering van de maatregel natuurlijk complexer worden en ook 'subjectiever' voor de autoriteit die ermee zou belast zijn. Om moeilijkheden bij de interpretatie van het toepassingsgebied van de maatregel te voorkomen, zouden deze punten in de tekst ook moeten worden verduidelijkt.

3.2.2. Aangaande de maatregelen die technisch en juridisch het voorwerp kunnen uitmaken van een bevel

3.2.2.1. De efficiëntie van de ten uitvoer gebrachte maatregelen

61. Het zou (zo goed als) niet efficiënt zijn om een beperking van digitale toegang in te voeren die begrensd zou blijven tot het verwijderen van een gebruikersaccount gecreëerd in naam van de betrokken entiteit (rechtspersoon of feitelijke vereniging of eenvoudige groepering), zonder enige andere maatregel die moet voorkomen dat dezelfde entiteit onmiddellijk een nieuwe account maakt, in voorkomend geval onder een andere gebruikersnaam of pseudoniem.
62. Om elke poging tot heropduiken van de betreffende entiteit doeltreffend te voorkomen, zouden betrouwbare technische middelen het mogelijk moeten maken om de natuurlijke personen die in naam van deze betreffende entiteit handelen te identificeren, niet alleen aan de hand van haar oorspronkelijke gebruikersaccount, maar ook aan de hand van haar latere activiteiten. In dit verband houdt de invoering van een maatregel ter beperking van digitale toegang rechtstreeks verband met deze van de betrouwbare identificatie van gebruikers van diensten, en het omgekeerde daarvan, nl. online anonimiteit.
63. Hoewel het voorontwerp stelt dat de maatregel geen individuen beoogt, maar enkel de groeperingen (*a fortiori* wanneer deze geen rechtspersoonlijkheid hebben) waarvan ze deel uitmaken, kan niet anders dan geconcludeerd worden dat het toezicht op de activiteiten van de individuen een relevant element lijkt voor de daadwerkelijke tenuitvoerlegging van de maatregel.²⁹ Als de activiteit van de individuen niet wordt gevolgd, lijkt de tenuitvoerlegging enkel mogelijk door monitoring van de inhoud, om inhoud afkomstig van diezelfde entiteit op te sporen wanneer die opnieuw verschijnt.

²⁹ Zie met name [advies nr. 52.522 van de Raad van State van 19 februari 2013](#), dat aangaande feitelijke verenigingen zoals private militias bepaalt dat "*het nu eenmaal niet mogelijk [is] iets te ontbinden wat in rechte niet bestaat als rechtssubject*" (punt 25, blz. 16). Het advies stelt verder: "*(...) alhoewel de eerder vermelde strafwetten - expliciet of impliciet - verenigingen viseren zoals private militias (...) zij er wezenlijk slechts toe strekken de personen aan te wijzen die, omwille van hun betrokkenheid bij die vereniging, strafrechtelijk aanspreekbaar zijn (...).*" (punt 27, blz. 17). In dit geval kan een soortgelijke redenering worden gevolgd met betrekking tot de toepassing van een maatregel ter beperking van de digitale toegang.

64. Verder dient te worden opgemerkt dat de efficiëntie van een maatregel ter beperking van digitale toegang van een dienst aanbieder die in een andere lidstaat is gevestigd, sterk afhangt van het bestaan van passende Europese of zelfs internationale samenwerkingsmechanismen. Daarom tracht de DSA een kader te bieden voor de bevelen om op te treden tegen specifieke inhoud of verstrekking van specifieke informatie over gebruikers die worden uitgevaardigd door nationale autoriteiten, door te voorzien in bepaalde vormelijke vereisten en procedurele verplichtingen voor de behandeling van dergelijke bevelen. Het doel is de daadwerkelijke en efficiënte uitvoering van deze bevelen te garanderen, in het bijzonder wanneer ze een grensoverschrijdende dimensie hebben, binnen een context waarin de nationale wetgeving waarop ze berusten aanzienlijk kan verschillen van de ene lidstaat tot de andere. Bij gebrek aan een onder aanbieders gecoördineerd mechanisme, zou de maatregel ter beperking van digitale toegang er eenvoudigweg toe kunnen leiden dat de betreffende gebruiker overstapt naar andere diensten, waardoor deze maatregel in de praktijk aan efficiëntie verliest. Dat is des te meer het geval daar de meerderheid van de dienst aanbieders die dit voorontwerp lijkt te beogen, niet in België zijn gevestigd, en soms zelfs niet in Europa. In overeenstemming met de DSA en de RTCO moeten deze daarentegen in een dergelijk geval een wettelijke vertegenwoordiger aanwijzen in een van de lidstaten, die dan bevoegd is voor de tenuitvoerlegging van de DSA en/of de RTCO.
65. Dit ontwerp zou dus een nationaal mechanisme beogen in te voeren dat parallel loopt met dat van de DSA en de RTCO, zonder te zorgen voor de middelen voor een daadwerkelijke grensoverschrijdende tenuitvoerlegging.

3.2.2.2. De noodzakelijke en evenredige aard van de ten uitvoer gebrachte maatregelen

66. Op basis van het derde en het vierde lid van artikel 5, § 3, zullen de autoriteiten en diensten belast met de uitvoering en de follow-up van de maatregelen ter beperking van digitale toegang over een erg grote flexibiliteit beschikken wat betreft de aard van de uit te vaardigen bevelen en de geadresseerden ervan, voor zover deze "strikt noodzakelijk" zijn voor de daadwerkelijke uitvoering van deze maatregel.
67. In zijn huidige vorm geeft de ontwerp tekst geen verdere verduidelijking over de soorten maatregelen (andere dan het louter blokkeren van de oorspronkelijke account van de betrokken entiteit bij de betreffende dienst aanbieder) die het voorwerp zouden kunnen uitmaken van een bevel³⁰, en evenmin over de geadresseerden daarvan, die zich derhalve waarschijnlijk zouden kunnen uitstrekken tot een bredere kring dan alleen de dienst aanbieders waarop het verbod betrekking heeft.
68. In deze context zou een maximalistische interpretatie van de ontwerp tekst inhouden dat, in het geval dat de dienst aanbieder – bijvoorbeeld een onlineplatform waarvan het gebruik voor bepaalde gebruikers zou zijn verboden – zich niet zou schikken naar de bevelen tot beperking van digitale toegang, de bevoegde autoriteit bijvoorbeeld internetproviders (ISP's)³¹ zou kunnen verplichten de toegang tot die dienst op het Belgische grondgebied te blokkeren. Een dergelijke maatregel houdt echter in dat de toegang tot de dienst niet alleen wordt ontzegd aan de gebruiker(s) beoogd door de maatregel ter beperking van

³⁰ Het is bijvoorbeeld niet duidelijk welke de "materiële" of "technische" handelingen zijn die strikt noodzakelijk zouden zijn voor de uitvoering van de maatregel ter beperking van digitale toegang.

³¹ Die tegelijk onder het begrip "**aanbieders van tussenhandeldiensten**" vallen in de zin van artikel 3, lid 1, punt g), i) van de DSA en het begrip "**aanbieder van elektronischemediatiediensten**" in de zin van artikel 2, 4) van het Europees wetboek voor elektronische communicatie.

digitale toegang, maar aan alle gebruikers van die dienst op het Belgische grondgebied. Een dergelijke maatregel lijkt dan ook moeilijk verenigbaar met de evenredigheidsvereiste.

69. Bovendien roept het voorbehouden van een dergelijke beoordelingsmarge met betrekking tot de noodzaak en de evenredigheid van maatregelen die mogelijk zo ingrijpend zijn voor de betrokken grondrechten, ook fundamentele vragen op vanuit het oogpunt van de naleving van het legaliteitsbeginsel.³²

³² In dit verband verwijzen we met name naar de overwegingen geuit in het kader van [Advies nr. 2025/9 van 18 september 2025 van het Federaal Instituut voor de bescherming en de bevordering van de Rechten van de Mens](#).

4. Conclusie

70. Aangaande het voorontwerp van wet betreffende het administratief verbod op de activiteiten van rechtspersonen, vennootschappen zonder rechtspersoonlijkheid, en feitelijke verenigingen of groeperingen die een ernstige en actuele bedreiging vormen voor de nationale veiligheid, blijkt uit het voorgaande dat het BIPT niet over de bevoegdheden beschikt die noodzakelijk zijn voor de tenuitvoerlegging van dit ontwerp.
71. Als regulator voor de digitale sector, met name in het kader van de DSA en de RTCO, heeft het BIPT de bevoegdheid om bepaalde voor de digitale tussenhandeldiensten opgelegde zorgvuldigheidsverplichtingen te doen naleven, zonder dat het echter gemachtigd is te oordelen over de illegaliteit van de inhoud die via deze diensten wordt verspreid. Zorgen voor een 'eventuele aanvullende wettelijke grondslag' zou niet louter een uitbreiding van de bestaande opdrachten van het BIPT inhouden, maar zou van die aard zijn dat het BIPT een rol toegekend krijgt die duidelijk buiten zijn huidige opdrachten valt, zelfs als regulator van de digitale sector. Dit zou er namelijk toe leiden dat het BIPT zou moeten optreden in aangelegenheden op het gebied van de nationale veiligheid, die onder de bevoegdheid vallen van andere autoriteiten die over de daarvoor benodigde expertise beschikken.
72. Hieronder volgen de voornaamste bedenkingen met betrekking tot het beoogde mechanisme en in het bijzonder de administratieve maatregel ter beperking van digitale toegang, bedoeld in artikel 5, § 1, 1°, d), van het eerste voorontwerp van wet.
73. *Ten eerste* zou duidelijker moeten worden gepreciseerd welke aanbieders en diensten betrokken zijn, om alle dubbelzinnigheid weg te nemen over de reikwijdte van de beoogde maatregel.
74. *Ten tweede* zouden de uitvoeringsmaatregelen en de geadresseerden daarvan moeten vastgelegd worden in de wet, rekening houdend met de vereisten van noodzakelijkheid en evenredigheid, maar ook beperkingen in termen van efficiëntie van die maatregelen. In dat opzicht zou rekening moeten gehouden worden met de Europese wettelijke context (DSA, RTCO en andere lopende initiatieven), evenals met de praktische moeilijkheden die voortvloeien uit het feit dat de betrokken dienstaanbieders niet op het Belgische grondgebied aanwezig zijn.
75. Wat betreft het voorontwerp van wet *betreffende de beroepen bij de Raad van State tegen de administratieve verbodsmaatregelen waarin is voorzien bij de wet van XXX betreffende het administratief verbod op de activiteiten van bepaalde entiteiten die een ernstige en actuele bedreiging vormen voor de nationale veiligheid*, zou dit, indien dit inderdaad gepaard zou gaan met een aanvullende wettelijke grondslag die het BIPT een rol als administratieve autoriteit toekent, tot gevolg hebben dat eenzelfde actor, namelijk een dienstenaanbieder die onderworpen is aan verschillende regelgevingen die onder de bevoegdheid van het BIPT vallen, afhankelijk van het soort geschil in kwestie een verschillend rechtsmiddel zou moeten gebruiken.

Bernardo Herman
Lid van de Raad

Peggy Valcke
Lid van de Raad

Stefaan Vyverman
Lid van de Raad

Michel Van Bellinghen
Voorzitter van de Raad