FEDERALE OVERHEIDSDIENST BELEID EN ONDERSTEUNING

[C − 2024/001452]

Omzendbrief van de minister van Telecommunicatie over de verstrekking van gegevens bewaard op grond van de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie door de operatoren aan de bevoegde Belgische autoriteiten

SERVICE PUBLIC FEDERAL STRATEGIE ET APPUI

[C − 2024/001452]

Circulaire de la ministre des Télécommunications concernant la fourniture par les opérateurs aux autorités belges compétentes de données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques

Inhoudsopgave

1. Samenvatting

1. De minister van Telecommunicatie dient in het Belgisch Staatsblad een omzendbrief te laten publiceren die een lijst omvat "*met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127*" van de wet van 13 juni 2005 betreffende de elektronische communicatie. Die lijst is terug te vinden in de bijlage. De autoriteiten op deze lijst hebben een fiche met meer informatie opgesteld. Deze fiches zijn gepubliceerd op de website van het BIPT. Dit document omvat ook algemene beschouwingen betreffende de verzoeken van de autoriteiten en de uitvoering ervan door de operatoren.

2. Voorwerp

2. Dit document is de omzendbrief die de minister van Telecommunicatie[1] moet bekendmaken in het Belgisch Staatsblad overeenkomstig artikel 127/1, § 5, tweede lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de wet betreffende de elektronische communicatie). Dit artikel werd ingevoegd in deze wet bij de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (hierna de wet gegevensbewaring van 2022).

3. Artikel 127/1, § 5, tweede lid, van de wet betreffende de elektronische communicatie schrijft voor dat de omzendbrief "*een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127*" van diezelfde wet. Die lijst is terug te vinden in de bijlage. Meer gedetailleerde informatie is te vinden in de fiches gepubliceerd op de website van het BIPT[2]. Deze fiches zijn opgesteld door de autoriteiten die in de bijlage bij dit document werden opgelijst.

4. Deze omzendbrief omvat ook algemene beschouwingen die bestemd zijn om de operatoren[3] en de bevoegde Belgische autoriteiten te helpen in het kader van een verzoek om gegevens die worden bewaard op grond van een van de voormelde artikelen.

5. Een operator heeft verzocht om in deze omzendbrief een lijst op te nemen van de autoriteiten die operatoren kunnen verzoeken om bestaande gegevens te bevriezen (quick freeze) of toekomstige gegevens te bevriezen (future freeze).

6. Het is echter niet de wet betreffende de elektronische communicatie die voorziet in deze vorm van gegevensbewaring (quick freeze en future freeze), maar wel de wetgeving van de verzoekende autoriteiten. Daarom vermeldt deze omzendbrief hieronder, uitsluitend ter informatie, de Belgische autoriteiten die dergelijke verzoeken aan de operatoren kunnen

[1] Volgens artikel 127/1, § 5, tweede lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie, is het de taak van de minister om deze omzendbrief bekend te maken in het Belgisch Staatsblad. Artikel 2, 2°, van diezelfde wet definieert het begrip "minister" als *"de ministers of staatssecretaris die bevoegd zijn voor de aangelegenheden die de elektronische communicatie betreffen als bedoeld in deze wet*".
[2] https://www.bipt.be/operatoren/wettelijke-onderschepping.
[3] Artikel 2, 11°, van de wet betreffende de elektronische communicatie definieert een operator als een "*persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt.*"

richten, aangezien meer informatie is opgenomen in de fiches die op de website van het BIPT zijn gepubliceerd:

6.1. De gerechtelijke autoriteiten op basis van de artikelen 39ter tot 39quinquies van het Wetboek van Strafvordering;

6.2. De inlichtingen- en veiligheidsdiensten op basis van artikel 13/6 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

6.3. De FSMA op basis van artikel 81, § 1bis en artikel 84, § 1bis/1 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten.

7. Naast de bekendmaking in het Belgisch Staatsblad zal deze omzendbrief ook gepubliceerd worden op de website van het BIPT[4]. Wijzigingen van dit document of de bijlage zullen op dezelfde wijze worden bekendgemaakt.

8. Deze omzendbrief is interpretatief en bestemd voor de operatoren en voor de Belgische autoriteiten die van een operator gegevens kunnen ontvangen die bewaard worden krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127 van de wet betreffende de elektronische communicatie.

3. Begrippen

Verschillende soorten van gegevens

9. Artikel 3, 9) van Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure (hierna de verordening inzake elektronisch bewijsmateriaal in strafzaken genoemd)[5] definieert "**abonneegegevens**" als "*gegevens die in het bezit zijn van een dienstaanbieder in het kader van een abonnement op zijn diensten en die betrekking hebben op:*

a) de identiteit van een abonnee of klant, zoals opgegeven naam, geboortedatum, postadres of geografisch adres, facturatie- en betalingsgegevens, telefoonnummer of e-mailadres;

b) de aard en de duur van de dienst, met inbegrip van technische gegevens en gegevens ter identificatie van gerelateerde technische maatregelen of interfaces die op het moment van de initiële registratie of activering worden gebruikt door of verstrekt aan de abonnee of klant, en gegevens met betrekking tot de validering van het gebruik van de dienst, met uitzondering van wachtwoorden of andere authenticatiemiddelen die in plaats van een wachtwoord worden gebruikt en door een gebruiker worden verstrekt of op zijn of haar verzoek worden gecreëerd."

10. In verschillende Europese wetgevingen wordt verwezen naar het begrip **verkeersgegevens**:

[4] https://www.bipt.be/operatoren/wettelijke-onderschepping.
[5] PB L 191/118 van 28.07.2023.

10.1. Artikel 2, lid 2, b), van de richtlijn betreffende privacy en elektronische communicatie[6] definieert "verkeersgegevens" als "*b) gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan*";

10.2. Artikel 3, 11) van de verordening inzake elektronisch bewijsmateriaal in strafzaken definieert "verkeersgegevens" als "*gegevens in verband met de verlening van een door een dienstaanbieder aangeboden dienst, die dienen om achtergrondinformatie of aanvullende informatie over die dienst te verstrekken en door een informatiesysteem van de dienstaanbieder zijn gegenereerd of verwerkt, zoals de herkomst en de bestemming van een bericht of een ander type interactie, de locatie van het apparaat, de datum, het tijdstip, de duur, de omvang, de route, de vorm, het gebruikte protocol en het type compressie, en andere elektronischecommunicatiemetagegevens, en gegevens, andere dan abonneegegevens, betreffende de aanvang en beëindiging van een toegangssessie van een gebruiker tot een dienst, zoals de datum en het tijdstip van het gebruik, het inloggen in en het uitloggen uit de dienst*."

11. Artikel 9 van de richtlijn betreffende privacy en elektronische communicatie (omgezet in artikel 123 van de wet betreffende de elektronische communicatie) heeft betrekking op de verwerking door operatoren van "**andere locatiegegevens dan verkeersgegevens**". Dit zijn locatiegegevens die nodig zijn voor de werking van het netwerk, maar die geen verband houden met de communicatie van inhoud.

12. Artikel 2, 93°, van de wet betreffende de elektronische communicatie definieert **"elektronische-communicatiemetagegevens"** als "*de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.*" Deze definitie is overgenomen uit de ontwerpverordening inzake privacy en elektronische communicatie, die door de Europese Commissie werd voorgesteld ter vervanging van de richtlijn betreffende privacy en elektronische communicatie[7].

13. Het begrip **inhoud** wordt gedefinieerd in verschillende wetten:

13.1. Artikel 3, 12), van de verordening inzake elektronisch bewijsmateriaal in strafzaken definieert "inhoudelijke gegevens" als "*gegevens die in digitale vorm zijn opgeslagen, zoals tekst, spraak, video's, beelden en geluid, en die geen abonneegegevens of verkeersgegevens zijn*";

13.2. Artikel 2, 92°, definieert "elektronische-communicatie-inhoud" als "*de uitgewisselde inhoud door middel van elektronische-communicatiediensten, zoals tekst, spraak, video, beelden en geluid*";

14. Artikel 3, 8), van de verordening inzake elektronisch bewijsmateriaal groepeert de verschillende categorieën gegevens onder het begrip "**elektronisch bewijsmateriaal** ":

[6] 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).

[7] Proposal of 10.1.2017 of the European Commission for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

"*abonneegegevens, verkeersgegevens of inhoudelijke gegevens die door of namens een dienstaanbieder in elektronische vorm zijn opgeslagen op het tijdstip van ontvangst van een certificaat inzake het Europees verstrekkingsbevel (CEV) of van een certificaat inzake het Europees bewaringsbevel (CEB)*".

15. De verschillende soorten gegevens verhouden zich onderling als volgt.

16. De begrippen 'verkeersgegevens' in de zin van de richtlijn betreffende privacy en elektronische communicatie en 'metagegevens' in de zin van de wet betreffende de elektronische communicatie zijn gelijkaardig. De volgende verschillen moeten echter worden opgemerkt:

16.1. Het begrip 'metagegevens' omvat niet de verkeersgegevens die nodig zijn voor de facturering (bijvoorbeeld de naam en het (e-mail)adres van de abonnee om de factuur te verzenden) en die niet beantwoorden aan de definitie van metagegevens;

16.2. Het begrip 'metagegevens' omvat de andere locatiegegevens dan verkeersgegevens, aangezien het begrip 'metagegevens' ook betrekking heeft op *"gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd"*.

17. De verkeers- of metagegevens zijn geen inhoudelijke elektronische-communicatiegegevens.

18. De artikelen 126 en 127 van de wet betreffende de elektronische communicatie verplichten de operatoren gegevens te bewaren met het uiteindelijke doel de eindgebruiker te identificeren. Dat sluit echter niet uit dat artikel 126 verkeersgegevens (of metagegevens) kan bevatten. Volgens artikel 126, § 1, 15°, moeten de operatoren het IP-adres aan de bron van de verbinding bewaren en volgens de rechtspraak van het HvJ-EU maken IP-adressen deel uit van de verkeersgegevens[8].

19. Het feit dat de IP-adressen nuttig kunnen zijn om de eindgebruiker te identificeren, komt tot uiting in de definitie van "gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker" in artikel 3, 10), van de verordening inzake elektronisch bewijsmateriaal in strafzaken: "*IP-adressen en, indien nodig, de relevante bronpoorten en tijdstempel, met name de datum en het tijdstip, of de technische equivalenten van die identificatoren alsook daarmee verband houdende informatie, wanneer rechtshandhavingsinstanties of rechterlijke autoriteiten hierom verzoeken met als enig doel de gebruiker te identificeren in het kader van een specifiek strafrechtelijk onderzoek*".

20. De gegevens die de operatoren krachtens de artikelen 126/1 tot 126/3[9] van de wet betreffende de elektronische communicatie (gerichte bewaring op geografische basis) moeten bewaren, zijn verkeersgegevens (of metagegevens).

Begrip van verzoek

21. In dit document wordt het begrip "verzoek" gebruikt om te verwijzen naar de formele vraag van een autoriteit aan een operator om gegevens bewaard op grond van de artikelen 122,

[8] HvJ-EU, arrest *"La Quadrature du Net"*, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, punt 152.
[9] Artikel 127/1, § 5, van de wet betreffende de elektronische communicatie, die de juridische grondslag vormt voor deze omzendbrief, beoogt de artikelen 126/1 en 126/3. In werkelijkheid zijn het de artikelen 126/1, 126/2 en 126/3 die betrekking hebben op de gerichte bewaring op geografische basis en de in dit verband te bewaren gegevens zijn opgenomen in artikel 126/2, § 2.

123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie te verstrekken. In de praktijk kan het verzoek van een autoriteit een andere naam dragen (bijvoorbeeld de vordering of het verzoekschrift).

4. De materiële bevoegdheid van de autoriteit die de gegevens eist

Overzicht van de twee voorwaarden die vermeld zijn in artikel 127/1 van de wet betreffende de elektronische communicatie

22. De paragrafen 2 tot 4 van artikel 127/1 van de wet betreffende de elektronische communicatie luiden als volgt:

"*§ 2. Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm:*

1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het vrijwaren van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.
Enkel de autoriteiten bedoeld in paragraaf 2 mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127, voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.
In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.
In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.
§ 4. De gegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1° tot 3° en 6°.
Enkel de in paragraaf 2, 1° tot 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens de artikelen 126/1 en 126/3 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm."

23. Deze paragrafen beogen het geval waarin een Belgische autoriteit van een operator eist dat deze laatste haar persoonsgegevens verstrekt die bewaard worden op grond van de artikelen 122, 123, 126, 126/1, 126/3 of 127 van de wet betreffende de elektronische communicatie.

24. In de memorie van toelichting bij de wet gegevensbewaring van 2022 staat dat artikel 127/1 van de wet betreffende de elektronische communicatie niet van toepassing is "*op de situaties waarin de gegevens worden verzonden naar een autoriteit door een van de bij de communicatie betrokken partijen of worden gevraagd door een autoriteit aan een van deze partijen. Tot deze laatste hypothese behoort met name de situatie waarin een partij haar metagegevens doorstuurt naar een autoriteit met het oog op een klacht, een geschillenbeslechting of een ambtshalve verzoek*[10]." (blz. 96)

25. Deze situatie komt eveneens voor in artikel 122, § 6, van de wet betreffende de elektronische communicatie, dat het volgende bepaalt: "*Het Instituut, de Raad voor de Mededinging, de rechtscolleges van de rechterlijke orde en de Raad van State kunnen in het kader van hun bevoegdheden in kennis worden gesteld van de relevante verkeers- en rekeninggegevens met het oog op het beslechten van geschillen, waaronder geschillen met betrekking tot interconnectie en facturering.*"

26. Deze bepaling vormt geen wettelijke grondslag aan de hand waarvan deze verschillende autoriteiten gegevens, bewaard op grond van de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie, van operatoren kunnen verlangen, maar verwijst naar de situatie waarin een van bij de communicatie betrokken partijen (die, indien van toepassing, de operator zelf kan zijn) gegevens aan de autoriteit verstrekt.

27. Voorts bepaalt de toelichting bij de wet gegevensbewaring van 2022 dat artikel 127/1 van de wet betreffende de elektronische communicatie evenmin van toepassing is: "*wanneer een*

[10] Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, Parl. St, Kamer, 2021-2022, nr. 2572/001.

operator anonieme gegevens verzendt naar een derde. De gegevens moeten anoniem gemaakt worden overeenkomstig de eisen van de AVG en moeten anoniem gemaakt worden ten aanzien van natuurlijke personen en rechtspersonen op wie deze gegevens betrekking hebben (en niet alleen ten aanzien van de natuurlijke personen zoals het geval is in de AVG). De richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58) beschermt immers de vertrouwelijkheid van de gegevens die verband houden met zowel rechtspersonen als natuurlijke personen." (blz. 96)

28. Uit artikel 127/1 blijkt dat een operator gegevens die bewaard worden op grond van de artikelen 126, 126/1, 126/3 of 127, namelijk gegevens die voor de autoriteiten worden bewaard, niet voor zijn eigen behoeften mag gebruiken. Dit principe doet geen afbreuk aan de mogelijkheid voor een operator om, binnen de voorwaarden bepaald in de wet (zie in het bijzonder artikelen 122 en 123 van de wet betreffende de elektronische communicatie), gegevens te bewaren voor zijn eigen behoeften of in het belang van zijn klanten.

29. Overeenkomstig artikel 127/1, §§ 2 tot 4, van de wet betreffende de elektronische communicatie, mag een operator persoonsgegevens die bewaard worden op grond van de artikelen 122, 123, 126, 126/1, 126/3 of 127 van de wet betreffende de elektronische communicatie, niet aan een derde meedelen, tenzij in de gevallen waarin artikel 127/1 voorziet en die hieronder worden uiteengezet.

30. Zoals blijkt uit artikel 127/1 van de wet betreffende de elektronische communicatie en uit de memorie van toelichting van de wet gegevensbewaring van 2022 moet een Belgische autoriteit die van een operator verlangt dat deze laatste haar persoonsgegevens verstrekt die bewaard worden op grond van de artikelen 122, 123, 126, 126/1, 126/3 of 127 van de wet betreffende de elektronische communicatie, voldoen aan de volgende twee cumulatieve voorwaarden:

30.1. zij moet beantwoorden aan een van de doeleinden beoogd in artikel 127/1[11], en;

30.2. een formele wettelijke norm moet haar bevoegd verklaren om die gegevens van de operator te eisen.

31. Hieronder wordt dieper ingegaan op die twee voorwaarden.

Eerste voorwaarde: beantwoorden aan een doeleinde van toegang tot de gegevens bedoeld in artikel 127/1 van de wet betreffende de elektronische communicatie

32. De autoriteit die van een operator verlangt dat deze laatste haar persoonsgegevens verstrekt die bewaard worden op grond van de artikelen 122, 123, 126, 126/1, 126/3 of 127 van de wet betreffende de elektronische communicatie moet voldoen aan een van de doeleinden waarvan sprake in artikel 127/1 van diezelfde wet.

33. De toegestane toegangsdoeleinden verschillen naargelang de gegevens, waartoe de autoriteit toegang heeft, worden bewaard op grond:

[11] Het begrip van toegang tot gegevens is terug te vinden in de rechtspraak van het HvJ-EU en vereenvoudigt de tekst, maar in de praktijk verstrekken de operatoren aan de autoriteiten de gevraagde gegevens.

33.1. van de artikelen 122 en 123 van de wet betreffende de elektronische communicatie (gegevens bewaard door de operatoren voor hun eigen behoeften of in het belang van hun klanten), of;

33.2. van de artikelen 126 en 127 van de wet betreffende de elektronische communicatie ((technische) gegevens met het oog op de identificatie van de eindgebruiker), of;

33.3. van de artikelen 126/1 tot 126/3 van de wet betreffende de elektronische communicatie (metagegevens bewaard in het kader van de doelgerichte bewaring op geografische basis).

34. In de onderstaande tabel is de exhaustieve lijst te zien van de toegangsdoeleinden die toegestaan zijn volgens het soort van bewaarde gegevens:

Alle toegangsdoeleinden en autoriteiten bedoeld in artikel 127/1, § 2	Toegestane toegangsdoeleinden afhankelijk van de verschillende soorten bewaarde gegevens		
	Gegevens art. 122 en 123[12]	Gegevens art. 126 en 127[13]	Gegevens art. 126/1 tot 126/3[14]
1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de wet houdende regeling van de inlichtingen- en veiligheidsdiensten[15]	Ja	Ja	Ja
2° de preventie van ernstige bedreigingen voor de openbare veiligheid	Ja	Ja	Ja
3° vrijwaren van de vitale belangen van natuurlijke personen	Ja	Ja	Ja
4° onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen	Ja	Ja	Neen
5° preventie, onderzoek, opsporing of vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische communicatienetwerk of –dienst	Ja	Ja	Neen
6° preventie, onderzoek, opsporing of vervolging van een feit dat onder de zware criminaliteit valt	Ja	Ja	Ja
7° vrijwaren van een belangrijk economisch of financieel belang van de EU of van België	Ja	Ja	Neen

[12] Zie artikel 127/1, § 2.
[13] Zie artikel 127/1, § 3. Artikel 127/1, § 3, derde lid bepaalt: "*In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.*"
[14] Zie artikel 127/1, § 4.
[15] De organieke wet houdende regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998.

8° preventie, onderzoek, opsporing of vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt	Ja	Ja	Neen
9° het BIPT in het kader van de controle van de wet betreffende de elektronische communicatie en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten	Ja	Ja	Ja
10° wetenschappelijk of historisch onderzoek of statistische doeleinden	Ja	Ja (behalve IP-adres)	Neen

35. Bijvoorbeeld "voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen" (toegangsdoeleinde opgenomen in artikel 127/1, § 2, 4°, van de wet betreffende de elektronische communicatie) stelt de bevoegde autoriteiten in staat te voldoen aan de eerste voorwaarde van artikel 127/1 (toegangsdoeleinde, cf. supra) voor de gegevens die door de operatoren worden bewaard overeenkomstig de artikelen 122, 123, 126 en 127, maar niet voor de gegevens die dezelfde operatoren overeenkomstig de artikelen 126/1 tot 126/3 bewaren (gegevens die op geografische basis worden bewaard).

36. Artikel 127/1, § 1, van de wet betreffende de elektronische communicatie bepaalt het volgende:

"*zware criminaliteit [omvat] met name de feiten waarvoor er ernstige aanwijzingen bestaan:*

1° dat ze de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88bis, § 1, eerste lid, van het Wetboek van strafvordering tot gevolg kunnen hebben;

2° dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht;

3° dat ze een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende machtsmisbruik) (sic) *en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124* (sic)*, 2003/125/EG en 2004/72/EG van de Commissie of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.*"

Tweede voorwaarde: de formele wettelijke norm

37. Een autoriteit die van een operator verlangt dat deze laatste haar persoonsgegevens verstrekt die bewaard worden op grond van de artikelen 122, 123, 126, 126/1 tot 126/3 of 127 van de wet betreffende de elektronische communicatie, moet ook over een formele wettelijke norm beschikken die haar bevoegd verklaart om die gegevens aan de operator te vragen. Bijvoorbeeld de autoriteiten die bevoegd zijn "voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen" (doeleinde van toegang, opgenomen in artikel 127/1, § 2, 4°, van de wet betreffende de elektronische communicatie) kunnen in de praktijk enkel toegang krijgen tot de gegevens bewaard door de operatoren conform de artikelen 122, 123, 126 en 127 op voorwaarde dat de organieke wet van deze autoriteiten daarin uitdrukkelijk voorziet en volgens de voorwaarden vastgelegd in deze wet.

38. Volgens de memorie van toelichting van de wet gegevensbewaring van 2022, moet de formele wettelijke norm "*minstens het niveau van een wet hebben: federale wet, decreet, ordonnantie, Europese Verordening, enz.*" (blz. 96)

39. Die formele wettelijke norm moet preciseren:

> "*- de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;*
> *— de categorieën van gegevens die mogen gevraagd worden;*
> *— de beoogde doeleinden;*
> *— de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.*" (art. 127/1, § 5, van de wet betreffende de elektronische communicatie).

40. Over die bepaling wordt in de memorie van toelichting van de wet gegevensbewaring van 2022 (blz. 115 en 116) de volgende toelichting gegeven:

"*Om elke interpretatie van de organieke of sectorale wetgeving waarop een autoriteit zich baseert om gegevens te verkrijgen van de operator, te vermijden, is het van essentieel belang dat die wetgeving voorziet in de machtiging van de autoriteit om de gegevens te verkrijgen van de operator (of een gelijkwaardige uitdrukking, aangezien dit begrip breder kan zijn dan het begrip van operator in de zin van de telecomwet) en zich niet beperkt tot een machtiging om gegevens te verkrijgen van gelijk welke persoon. Het is ook van essentieel belang dat deze wetgeving voorschrijft dat de autoriteit identificatiegegevens of metagegevens kan verkrijgen (of elke uitdrukking die beoogt de van de operator te verkrijgen gegevens te preciseren) en zich niet beperkt tot het bepalen dat de autoriteit gelijk welke nuttige informatie mag vragen [...] Deze omzendbrief mag geen autoriteiten opnemen die eenvoudigweg wettelijk gemachtigd zouden zijn om van economische spelers gelijk welke nuttige informatie te vragen.*"

41. Bovendien staat het HvJ-EU in zijn arrest La Quadrature du Net van 6 oktober 2020 (gevoegde zaken C-511/18, C-512/18 en C-520/18) toe dat de lidstaten aan de operatoren bepaalde maatregelen inzake gegevensbewaring opleggen "*mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.*" (dispositief van het arrest)

42. Het is de formele wettelijke norm die deze materiële en procedurele voorwaarden en de waarborgen tegen misbruik moet bevatten.

Lijst van de autoriteiten die verklaren aan beide voorwaarden te voldoen

43. De bijlage bij deze omzendbrief bevat een lijst van autoriteiten die verklaren aan beide voormelde voorwaarden te voldoen.

44. Het beoogde doel is om een zo volledig mogelijke lijst te hebben. Er moet echter worden opgemerkt dat deze werd opgesteld op basis van informatie die de betrokken autoriteiten aan het BIPT en aan de minister van Telecommunicatie hebben verstrekt. Het is dus niet mogelijk om de volledigheid ervan te garanderen.

45. Indien een autoriteit een operator om gegevens, bewaard op grond van de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie, verzoekt, maar niet in deze lijst is opgenomen, moet zij de operator meedelen dat zij wel degelijk aan de twee bovengenoemde voorwaarden voldoet: beantwoorden aan een van de toegangsdoeleinden zoals vastgelegd in artikel 127/1, §§ 2 tot en met 4 van de wet betreffende de elektronische communicatie en beschikken over een formele wettelijke norm die voldoet aan de vereisten van paragraaf 5, eerste lid, van hetzelfde artikel. Het loutere feit dat een autoriteit niet in deze lijst is opgenomen, rechtvaardigt evenwel niet dat de operator weigert gevolg te geven aan het door deze autoriteit aan hem gerichte verzoek.

46. Als aan een van deze voorwaarden niet wordt voldaan, moet de operator weigeren het verzoek uit te voeren. Indien aan beide voorwaarden is voldaan, moet de autoriteit in de bijgevoegde lijst opgenomen worden. Opdat deze lijst kan worden bijgewerkt om zo goed mogelijk de realiteit te weerspiegelen, wordt het volgende gevraagd:

46.1. elke autoriteit die niet is opgenomen in de lijst, maar die van mening zou zijn dat ze over de wettelijke bevoegdheden beschikt om erin opgenomen te worden, wordt verzocht dat te melden aan het BIPT en het kabinet van de minister van Telecommunicatie;

46.2. de betrokken autoriteiten worden zo ook verzocht om hen op de hoogte te brengen van elke wijziging in hun wetgeving die een aanpassing van deze lijst zou noodzaken.

47. Tot slot dient te worden herinnerd aan de louter interpretatieve aard van deze omzendbrief, die geen kracht van wet heeft, en wordt geformuleerd onder voorbehoud van de interpretatie van de hoven en rechtbanken.

5. De territoriale bevoegdheid van de autoriteit die de gegevens eist

48. Uit het arrest van 1 december 2015 (P.13.2082.N/1, YAHOO! Inc.) van het Hof van Cassatie van België vloeit voort dat een operator aan de Belgische wetgeving onderworpen is, alleen al door zijn actieve deelname aan het bedrijfsleven in België, en dat die dus een verzoek om gegevens vanwege de procureur des Konings moet inwilligen conform artikel 46bis van het Wetboek van Strafvordering:

"2. Artikel 46bis Wetboek van Strafvordering bepaalt:

- in paragraaf 1, eerste lid, dat de procureur des Konings bij het opsporen van misdaden en wanbedrijven, bij een gemotiveerde en schriftelijke beslissing de medewerking kan vorderen van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst teneinde de in die bepaling vermelde gegevens te verkrijgen;

- in paragraaf 2, eerste lid, dat iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie wordt gevorderd de in paragraaf 1 bedoelde gegevens mede te delen, deze verstrekt aan de procureur des Konings.

3. Die bepaling vermeldt in paragraaf 2, vierde lid, ook dat de weigering de

bedoelde gegevens mee te delen, wordt gestraft met een geldboete. Deze strafsanctie strekt ertoe de op de bedoelde operatoren en verstrekkers rustende medewerkingsverplichting af te

dwingen en geeft in zoverre aan artikel 46bis, § 2, Wetboek van Strafvordering het karakter van een dwangmaatregel.

4. In de regel kan een Staat enkel op zijn eigen grondgebied dwangmaatregelen nemen om de naleving van zijn wetten af te dwingen en eigent hij zich, zo hij een dergelijke maatregel neemt op het grondgebied van een andere Staat, een extraterritoriale rechtsmacht toe die de soevereiniteit van die Staat miskent.

5. Een Staat neemt een dwangmaatregel op zijn eigen grondgebied wanneer er tussen die maatregel en dat grondgebied een voldoende territoriaal aanknopingspunt bestaat. Welk territoriaal aanknopingspunt minstens vereist is, wordt onder meer bepaald door de aard en de draagwijdte van de dwangmaatregel.

6. De in artikel 46bis, § 2, vierde lid, Wetboek van Strafvordering bepaalde strafsanctie strekt enkel ertoe vanwege in België actieve operatoren en verstrekkers zoals hiervoor bedoeld, een maatregel af te dwingen die tot doel heeft loutere identificatiegegevens te verkrijgen naar aanleiding van een misdrijf waarvan de opsporing behoort tot de bevoegdheid van de Belgische strafrechtsmachten. Die maatregel vereist geen aanwezigheid in het buitenland van Belgische politieambtenaren of magistraten noch van personen die voor hen optreden. Evenmin vereist die maatregel het stellen van enige materiële handeling in het buitenland. Het betreft derhalve een dwangmaatregel met een beperkte draagwijdte, waarvan de uitvoering geen interventie buiten het Belgische grondgebied vereist.

7. Artikel 3 Strafwetboek bepaalt dat het misdrijf, op het grondgebied van het Rijk door Belgen of door vreemdelingen gepleegd, gestraft wordt overeenkomstig de bepalingen van de Belgische wetten. Het misdrijf, bepaald in artikel 46bis, § 2, vierde lid, Wetboek van Strafvordering, wordt gepleegd op de plaats waar de gevorderde gegevens moeten worden ontvangen. Bijgevolg is de operator of de verstrekker die weigert deze gegevens mee te delen, in België strafbaar ongeacht zijn plaats van vestiging.

8. Uit het voorgaande volgt, eensdeels, dat de maatregel die bestaat in de verplichting de hier bedoelde gegevens te verstrekken, wordt genomen op het Belgische grondgebied ten aanzien van elke operator of verstrekker die zijn economische activiteit actief op consumenten in België richt, anderdeels, dat de Belgische rechter die een in het buitenland gevestigde operator of verstrekker veroordeelt wegens het miskennen van deze verplichting en die aldus de naleving van een in België genomen maatregel afdwingt, geen extraterritoriale rechtsmacht uitoefent. In zoverre het middel uitgaat van een andere rechtsopvatting, faalt het naar recht.

9. Met overname van de redenen van het beroepen vonnis en met eigen redenen oordelen de appelrechters onder meer dat de eiseres, als verstrekker van een gratis webmaildienst, in België territoriaal aanwezig is en zich vrijwillig aan de Belgische wet onderwerpt omdat zij actief deelneemt aan het economische leven in België, onder meer door gebruik te maken van de domeinnaam "www.yahoo.be", het gebruik van de lokale taal, het tonen van reclame gebaseerd op de locatie van de gebruikers van haar diensten en haar bereikbaarheid in België voor die gebruikers via onder meer een klachtenbus en een vraagbaak. Met overname van de redenen van het beroepen vonnis (ro 4.2 en 4.4) oordelen de appelrechters ook dat:

- de procureur des Konings niets in de Verenigde Staten van Amerika vraagt aan een onderdaan van dat land, maar substantieel iets in België vraagt aan een in België aangetroffen dienstverlenende onderdaan van dat land;".

49. Diezelfde redenering is herhaald in het arrest van 19 februari 2019 (P.17.1229.N/1, Skype communications) van het Hof van Cassatie van België, maar dit keer voor een verzoek om de inhoud van een elektronische communicatie te verstrekken aan een onderzoeksrechter:

"*8. Artikel 88bis Wetboek van Strafvordering, zoals hier van toepassing, bepaalt:*

"§ 1. Wanneer de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van telecommunicatie of het lokaliseren van de oorsprong of de bestemming van telecommunicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij, zo nodig door daartoe de medewerking van de operator van een telecommunicatienetwerk of van de verstrekker van een telecommunicatiedienst te vorderen:

1° de oproepgegevens doen opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan;
2° de oorsprong of de bestemming van telecommunicatie laten lokaliseren.

In de gevallen bepaald in het eerste lid wordt voor ieder telecommunicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de telecommunicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.

De onderzoeksrechter vermeldt de feitelijke omstandigheden van de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings.

Hij vermeldt ook de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing.
[…]

§ 2. Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst deelt de gegevens waarom verzocht werd mee binnen een termijn te bepalen door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro".

Artikel 90quater, § 2, Wetboek van Strafvordering, zoals hier van toepassing, bepaalt:

"§ 2. Indien de maatregel een bewerking op een communicatienetwerk inhoudt, is de operator van dit netwerk of de verstrekker van de telecommunicatiedienst ertoe gehouden zijn technische medewerking te verlenen, wanneer de onderzoeksrechter hierom verzoekt.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro."

Die bepalingen laten de Belgische onderzoeksrechter toe om, in het kader van zijn gerechtelijk onderzoek, vanwege iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die zijn economische activiteit actief op consumenten in België richt, de hier bedoelde informatieverstrekking of technische bijstand te vorderen met betrekking tot in België gevoerde elektronische communicatie, ongeacht de

plaats waar die operator of verstrekker is gevestigd dan wel waar de infrastructuur ligt die vereist is om gevolg te geven aan de vordering van de onderzoeksrechter.

Eensdeels is een dergelijke operator of verstrekker immers onderworpen aan de Belgische wetgeving omwille van het enkele feit van zijn actieve deelname aan het economische leven in België.

Anderdeels vereist de hier bedoelde medewerkingsplicht geen interventie van de Belgische gerechtelijke overheid in het buitenland. Bijgevolg is de onderzoeksrechter niet ertoe gehouden een rechtshulpverzoek te richten aan de Staat waar die operator of vertrekker (sic) *zijn vestiging of infrastructuur heeft en is hij niet gebonden door de wetgeving van dat land.*"

6. De minimale vermeldingen van het verzoek gericht aan de operator

50. Artikel 127/1, § 6, van de wet betreffende de elektronische communicatie bepaalt het volgende:

"*De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127, omvatten de volgende minimale vermeldingen:*
1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;
2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;
3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;
4° de gewenste antwoordtermijn."

51. Het voormelde artikel 127/1, § 6, 3° bepaalt dat het verzoek het volgende moet bevatten: *"de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere".* De centrale dienst is in de praktijk de "NTSU", namelijk de *National Technical and Tactical Support Unit* van de speciale eenheden van de federale politie. Wanneer het verzoek om gegevens naar de operator wordt verzonden via de NTSU, voert de verzoekende autoriteit in de praktijk het verzoek om gegevens in het TANK-uitwisselingsplatform van de NTSU in[16]. In dat geval moet het verzoek (dat de wettelijke grondslag bevat) ook in dit platform worden ingevoerd.

52. De operator moet elk schriftelijk verzoek dat niet is ondertekend weigeren. Als de handtekening elektronisch is, moet deze voldoen aan de relevante wettelijke vereisten. Een handtekening onder een e-mail voldoet niet aan deze vereisten.

[16] Dit is een door de NTSU beheerd platform waarmee de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten bepaalde verzoeken om gegevens naar de operatoren kunnen verzenden en het antwoord van de operatoren kunnen ontvangen.

7. De interne of externe toetsing van het verzoek

53. In artikel 4 van de verordening inzake elektronisch bewijsmateriaal in strafzaken wordt een onderscheid gemaakt tussen:

- "*1. Een Europees verstrekkingsbevel voor het verkrijgen van abonneegegevens of gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker in de zin van artikel 3, punt 10)*[17]", en;

- "*2. Een Europees verstrekkingsbevel voor het verkrijgen van verkeersgegevens, met uitzondering van gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker zoals gedefinieerd in artikel 3, punt 10) [...]*".

54. Een soortgelijk onderscheid wordt teruggevonden in het Belgische recht. Het Wetboek van Strafvordering bepaalt aldus het volgende[18]:

" *46bis. § 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een met redenen omklede en schriftelijke beslissing overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de actoren bedoeld in het tweede lid, eerste en tweede streepje, tot:*
1° de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;
2° de identificatie van de diensten bedoeld in het tweede lid, tweede streepje, waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden." (wij onderlijnen)

"Art. 88bis. § 1. Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij:
1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;
2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren." (wij onderlijnen)

55. Dit onderscheid wordt ook weerspiegeld wat betreft de toetsing van het verzoek, zoals hieronder wordt uitgelegd.

---

[17] Artikel 3, punt 10) van die verordening definieert "gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker" als volgt: "IP-adressen en, indien nodig, de relevante bronpoorten en tijdstempel, met name de datum en het tijdstip, of de technische equivalenten van die identificatoren alsook daarmee verband houdende informatie, wanneer rechtshandhavingsinstanties of rechterlijke autoriteiten hierom verzoeken met als enig doel de gebruiker te identificeren in het kader van een specifiek strafrechtelijk onderzoek".

[18] Hetzelfde geldt voor de artikelen 81, § 1, eerste lid, en 84, § 1, eerste lid, van de wet betreffende het financiële toezicht (wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten), waarvan de gebruikte terminologie nagenoeg identiek is aan die van artikelen 46bis en 88 van het Wetboek van Strafvordering. Zie artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

56. Zoals geëist door de rechtspraak van het HvJ-EU[19] moet het verzoek van de autoriteit in geval van een verzoek om verkeersgegevens, met uitzondering van gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker en behalve in urgente gevallen, vooraf getoetst worden door een onafhankelijke administratieve autoriteit (bijvoorbeeld de Gegevensbeschermingsautoriteit) of door een rechterlijke instantie (bijvoorbeeld een onderzoeksrechter). In urgente gevallen moet de toetsing op korte termijn plaatsvinden. Deze (voorafgaande of latere) toetsing is een externe toetsing, aangezien de toetsing wordt uitgevoerd door een andere autoriteit dan de verzoekende persoon of autoriteit.

57. In geval van een verzoek om het verkrijgen van abonneegegevens of gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker, is deze externe toetsing niet vereist, maar is een interne toetsing (toetsing binnen de verzoekende autoriteit) noodzakelijk. Die interne toetsing omvat bijvoorbeeld een verificatie van de naleving van de formaliteiten (bijvoorbeeld de aanwezigheid van de vereiste handtekeningen, de verwijzing naar de wettelijke grondslag), van de noodzaak en van de evenredigheid van het verzoek. Die toetsing wordt bijvoorbeeld verricht door de procureur des Konings, door de aangestelde voor de bescherming van de persoonsgegevens (DPO of data protection officer), de verzoekende autoriteit, de hiërarchische meerdere of de speciaal daartoe aangewezen officier van gerechtelijke politie wat de wet met betrekking tot het statuut van het BIPT betreft[20].

58. Het is de organieke wetgeving van de verzoekende autoriteit die bepaalt welke toetsing (intern of extern) moet worden uitgevoerd, door wie en waaruit deze bestaat. Interne en externe toetsingen hebben betrekking op een toetsing door een autoriteit en niet op een toetsing door de operator.

59. Dit onderscheid tussen externe en interne toetsing vloeit voort uit het arrest "wet voorafbetaalde kaarten" van het Grondwettelijk Hof (arrest nr. 158/2021 van 18 november 2021):

> "*B.16.8.6. In dat verband verwijzen de verzoekende partijen naar het arrest van de grote kamer van het Hof van Justitie van 2 maart 2021 in zake Prokuratuur (C-746/18, punten 50 tot 56), waarin het Hof van Justitie volgens hen eist dat een onafhankelijke bestuurlijke autoriteit of een rechter elk verzoek tot toegang voorafgaandelijk toetst aan de toepasselijke nationale regels en grondrechten en waarin het volgens hen preciseert dat het openbaar ministerie, dat de onderzoeksprocedure leidt en in voorkomend geval optreedt als aanklager, niet over de vereiste onafhankelijkheid beschikt om die toetsing te kunnen doorvoeren.*
>
> *Dat arrest had evenwel betrekking op een verzoek van het openbaar ministerie om toegang te krijgen tot verkeers- en locatiegegevens. Zoals uiteengezet in B.14.3, vereisen het Hof van Justitie en het Europees Hof voor de Rechten van de Mens daarentegen geen voorafgaande rechterlijke of bestuurlijke toetsing van een verzoek om toegang tot identificatiegegevens. Bijgevolg verzet het recht op eerbiediging van het privéleven zich niet tegen een verzoek tot toegang tot dergelijke gegevens dat uitgaat van het openbaar ministerie.*" (wij onderlijnen)

[19] Arrest Digital Rights van 8 april 2014 (C-293/12), arrest Tele 2 van 21 december 2016 (C-203/15), arrest La Quadrature du Net van 6 oktober 2020 (C-511/18) en arrest Prokuratuur van 2 maart 2021 (C-746/18).
[20] Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

8. Verzoek gericht aan de coördinatiecel van de operator

60. Uit artikel 127/3, § 1, derde lid, van de wet betreffende de elektronische communicatie blijkt dat een autoriteit zich moet richten tot de coördinatiecel van de operator om gegevens bewaard op grond van de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie te krijgen.

61. Krachtens datzelfde artikel moet elke operator over zo'n cel beschikken.

62. Een Belgische autoriteit die nog niet over de contactgegevens van de wachtdienst van de coördinatiecel van de operatoren zou beschikken, kan zich wenden tot het BIPT om toegang tot die contactgegevens te krijgen.

63. Indien een verzoek gericht is tot een specifieke operator (en niet tot de operatoren in het algemeen), en het lijkt erop dat het gericht had moeten zijn aan een andere operator (bijvoorbeeld omdat het deze andere operator is die de informatie heeft over het in het verzoek beoogde telefoonnummer), dan zal de autoriteit een nieuw verzoek moeten richten tot deze operator.

9. Wat mag/moet de operator toetsen en in welke gevallen mag/moet hij een verzoek weigeren?

64. De operator moet controleren of het verzoek wel degelijk afkomstig is van de autoriteit die beweert zich tot hem te richten (en niet van een persoon die zich uitgeeft voor die autoriteit), tenzij het verzoek werd ingevoerd in het uitwisselingsplatform "TANK" van de NTSU. In dat geval wordt deze toetsing immers reeds uitgevoerd dankzij de technische toepassing en de functionele regels van dit platform. De operator moet weigeren het verzoek van de autoriteit uit te voeren indien de volgende minimale vermelding (zie titel 4 hierboven) in dat verzoek ontbreekt: "*1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;*".

65. De operator kan bepalen of het verzoek aan een interne of externe toetsing werd onderworpen door dat laatste te onderzoeken.

66. Wanneer uit het verzoek blijkt dat het aan externe toetsing (toetsing door een rechterlijke instantie of een onafhankelijke administratieve instantie) werd onderworpen, hoeft de operator geen aanvullende toetsing uit te voeren. Dat geldt ook wanneer die toetsing, wegens de urgentie, plaatsvindt na de verzending van het verzoek naar de operator.

67. Wanneer uit het verzoek blijkt dat het aan een interne toetsing werd onderworpen, wordt van de operator verwacht dat hij het verzoek controleert. Indien mogelijk wordt deze controle uitgevoerd voordat op het verzoek wordt gereageerd. De operator moet zich ervan vergewissen dat de wettelijke grondslag van het verzoek volstaat om de gegevens op te

vragen. Zo wordt in de memorie van toelichting van de wet gegevensbewaring van 2022 (zie blz. 116 en 117) het volgende vermeld: "*Alvorens gevolg te geven aan een verzoek om gegevens dat het voorwerp uitmaakt van een interne controle, is het de taak van de operator om na te gaan of de wettelijke basis aanwezig is die nodig is om de gegevens op te vragen*."

68. Een operator moet dus weigeren gevolg te geven aan een verzoek vanwege een autoriteit als dat niet op een toereikende wettelijke grondslag berust (zie hierboven "4. De materiële bevoegdheid van de autoriteit die de gegevens eist" en de twee voorwaarden waaraan moet worden voldaan). In de praktijk zal de operator eerst kunnen controleren of de wettelijke grondslag van het verzoek inderdaad in de bijlage bij dit document is vermeld. Als dat het geval is, dan volstaat de wettelijke grondslag in principe. Als dat niet het geval is, zal hij deze wettelijke grondslag nader moeten onderzoeken.

69. Een operator moet weigeren om aan een verzoek vanwege een autoriteit gevolg te geven als niet blijkt dat de interne of externe toetsing van het verzoek wel degelijk heeft plaatsgevonden (voorafgaande controle) of zal plaatsvinden (controle a posteriori in geval van urgentie).

70. Die controle blijkt uit het verzoek bijvoorbeeld als daarop is vermeld dat die is uitgevoerd of zal worden uitgevoerd (urgentie). Met andere woorden, de operator mag vertrouwen op de verklaring in het verzoek. Wanneer deze controle niet uit het verzoek blijkt en de operator dat meldt aan de verzoekende autoriteit, kan deze de operator ervan in kennis stellen dat deze controle wel degelijk is uitgevoerd (voorafgaande controle) of zal worden uitgevoerd (controle achteraf in geval van nood).

71. De operator kan echter niet weigeren het verzoek uit te voeren omdat hij geen kennis heeft kunnen nemen van de documenten die in het kader van interne of externe toetsing tussen de verschillende personen of autoriteiten zijn uitgewisseld.

72. Wanneer een operator weigert gevolg te geven aan een verzoek moet hij de verzoekende autoriteit daarvan op de hoogte brengen.

73. Zoals wordt uitgelegd in de memorie van toelichting van de wet gegevensbewaring van 2022 (zie blz. 116 en 117): "*Ongeacht of het gaat om een interne of een externe controle, is het [...] niet aan de operator om te oordelen over de evenredigheid van de verzoeken om gegevens van die autoriteit, noch om na te gaan of het verzoek voldoende gemotiveerd is*."

74. Zonder dat dit evenwel een argument vormt dat door de operator kan worden gebruikt om te weigeren zich naar het verzoek te schikken, belet niets de operator om aan de verzoekende autoriteit te laten weten dat dit verzoek volgens hem onevenredig is, omdat het een enorme werklast veroorzaakt, opdat die autoriteit zich bewust kan worden van de omvang van het verzoek en de evenredigheid ervan beter kan beoordelen.

10. De oplossingen in geval van een geschil tussen de operator en een Belgische autoriteit over een verzoek om gegevens

75. Het BIPT is niet bevoegd om een geschil tussen een operator en een autoriteit te beslechten. De rol van het BIPT beperkt zich ertoe:

75.1. aan een operator of aan een autoriteit, die het BIPT daarover een vraag stelt, de manier mee te delen waarop het van plan is de wet toe te passen;

75.2. de operator te controleren met betrekking tot een aantal bepalingen (bijvoorbeeld de wet betreffende de elektronische communicatie en de uitvoeringsbesluiten ervan, maar niet de organieke wetten van andere autoriteiten dan het BIPT of de Ombudsdienst voor telecommunicatie)[21].

76. Indien een geschil aanhoudt is het aan de hoven en rechtbanken om het geschil te beslechten.

77. Een operator kan niet worden gestraft voor het niet aan een autoriteit verstrekken van gegevens waarover hij niet beschikt (bijvoorbeeld als de operator geen identificatiegegevens heeft maar alleen abonnementsgegevens voor de dienst). De operator kan echter wel worden gestraft indien hij niet voldoet aan artikel 127 van de wet betreffende de elektronische communicatie wat betreft de identificatie van zijn abonnees, of indien hij de gegevens niet bewaart zoals bepaald in de artikelen 122, 123 en 126 tot en met 126/3.

11. Bijlage

78. Lijst met de Belgische autoriteiten die gemachtigd zijn om van een operator persoonsgegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet betreffende de elektronische communicatie.

Gegeven op

De Minister van Telecommunicatie

P. DE SUTTER

[21] De lijst van de bepalingen die door het BIPT worden gecontroleerd is te vinden in artikel 14, § 1, 3°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

Bijlage bij de omzendbrief: lijst met de Belgische autoriteiten die wettelijk gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123[22], 126, 127[23], 126/1 en 126/3[24] van de wet van 13 juni 2005 betreffende de elektronische communicatie (WEC)

Autoriteiten	Gegevens bewaard op basis van de art. 122 en 123 van de WEC	Gegevens bewaard op basis van de art. 126 en 127 van de WEC	Gegevens bewaard op basis van de art. 126/1 tot 126/3 van de WEC	Wettelijke basis
De gerechtelijke autoriteiten (procureur des Konings, onderzoeksrechter, Europese aanklager, gedelegeerde Europese aanklagers)	Ja	Ja	Ja, maar uitsluitend voor de feiten bedoeld in artikel 127/1, § 1, 1°, van de WEC (zware criminaliteit)[25]	Art. 46bis, 88bis, 464/13 en 464/25 van het Wetboek van Strafvordering. Zie ook art. 47quaterdecies van hetzelfde Wetboek wat betreft de Europese aanklagers.
Cel Vermiste Personen van de federale politie	Ja	Ja	Ja	Art. 42, § 2, van de wet van 5 augustus 1992 op het politieambt
De inlichtingen- en veiligheidsdiensten	Ja	Ja	Ja	Art. 16/2, 18/7, 18/8 en 18/17 van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998
De Belgische Mededingingsautoriteit (BMA)	Ja	Ja	Neen	Artikel IV.40, § 1/1, van het Wetboek van economisch recht
De Autoriteit voor Financiële diensten en Markten (FSMA)	Ja	Ja	Ja, maar uitsluitend voor de feiten bedoeld in artikel 127/1, § 1, van de WEC, onder meer deze bedoeld in	Art. 81, 82, 2° en 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

[22] Gegevens bewaard op basis van de artikelen 122 en 123: verkeers- en locatiegegevens bewaard door de operatoren voor hun eigen behoeften of in het belang van hun klanten.
[23] Gegevens bewaard op basis van de artikelen 126 en 127: gegevens (inclusief de IP-adressen) met het oog op de identificatie van de eindgebruiker.
[24] Gegevens bewaard op basis van de artikelen 126/1 tot 126/3: metagegevens bewaard in het kader van de doelgerichte bewaring op geografische basis.
[25] Het gaat om feiten waarvoor er ernstige aanwijzingen bestaan dat ze de lichtste correctionele hoofdgevangenisstraf bedoeld in artikel 88bis, eerste lid, van het Wetboek van Strafvordering tot gevolg kunnen hebben. Vanaf 4 september 2023 is deze minimumstraf één jaar gevangenisstraf.

Autoriteiten	Gegevens bewaard op basis van de art. 122 en 123 van de WEC	Gegevens bewaard op basis van de art. 126 en 127 van de WEC	Gegevens bewaard op basis van de art. 126/1 tot 126/3 van de WEC	Wettelijke basis
			artikel 127/1, § 1, 3°[26] (zware criminaliteit)	
De dienst Inspectie van het Directoraat-generaal Dier, Plant en Voeding van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu	Ja, uitsluitend voor identificatiedoeleinden	Ja	Neen	Art. 11, § 1, van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten (sic)
De Ombudsdienst voor telecommunicatie	Ja, uitsluitend voor identificatiedoeleinden	Ja	Neen	Art. 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven
De volgende inspectiediensten van de FOD Economie: - AD Energie (E2); - AD Kwaliteit en Veiligheid (E6); - AD Economische Inspectie (E7)	Ja Om verkeers- en locatiegegevens en de IP-adressen te verkrijgen: uitsluitend voor de feiten bedoeld in artikel 127/1, § 1, 2°, van de WEC (zware criminaliteit)[27]	Ja Om de IP-adressen te verkrijgen: uitsluitend voor de feiten bedoeld in artikel 127/1, § 1, 2°, van de WEC (zware criminaliteit)[28]	Ja, maar uitsluitend voor de feiten bedoeld in art. 127/1, § 1, 2°, van de WEC (zware criminaliteit)[29]	Art. XV.3, 5°/1, van het Wetboek van economisch recht
De officieren van gerechtelijke politie (OGP) van het Belgisch Instituut	Ja	Ja	Ja, maar uitsluitend in het kader van de controle op de	Art. 25/ 1 van de wet van 17 januari 2003 met betrekking tot het statuut van de

[26] Het gaat om feiten die een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende marktmisbruik) en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124/EG, 2003/125/EG en 2004/72/EG van de Commissie of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.
[27] Het gaat om feiten waarvoor er ernstige aanwijzingen bestaan dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht.
[28] Idem.
[29] Idem.

Autoriteiten	Gegevens bewaard op basis van de art. 122 en 123 van de WEC	Gegevens bewaard op basis van de art. 126 en 127 van de WEC	Gegevens bewaard op basis van de art. 126/1 tot 126/3 van de WEC	Wettelijke basis
voor postdiensten en telecommunicatie (BIPT)			naleving van de WEC door de operator	regulator van de Belgische post- en telecommunicatiesector
Het BIPT dat optreedt in het kader van een administratieve procedure	Ja	Ja	Ja, maar uitsluitend in het kader van de controle op de naleving van de WEC door de operator	Art. 15 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector
Het Centrum voor Cybersecurity België (CCB)[30]	Ja	Ja	Ja	Art. 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid
De Algemene Directie Statistiek - Statistics Belgium van de FOD Economie, KMO, Middenstand en Energie	Gegevens met betrekking tot de toegang, het gebruik en de financiële toegankelijkheid van de elektronische-communicatiediensten. Gegevens: - identiteit van de persoon die het contract heeft gesloten (naam en adres of rijksregisternummer); - identiteit van de onderneming die het contract heeft gesloten (naam en adres of KBO-nummer of btw-nummer); - identiteit van de persoon of de onderneming aan wie de factuur wordt geadresseerd; - het bedrag van de factuur; - de periode waarop de gefactureerde diensten betrekking hebben;		Neen	Artikel 24*sexies* van de wet van 4 juli 1962 betreffende de openbare statistiek

[30] In de hoedanigheid van nationale CSIRT in de zin van artikel 7, § 2, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Autoriteiten	Gegevens bewaard op basis van de art. 122 en 123 van de WEC	Gegevens bewaard op basis van de art. 126 en 127 van de WEC	Gegevens bewaard op basis van de art. 126/1 tot 126/3 van de WEC	Wettelijke basis
	- de verdeling van de kosten per dienst (vast internet, mobiel internet, vaste telefonie, mobiele telefonie en digitale televisie); - informatie over het type van aansluiting in termen van mogelijke snelheid (uitsluitend voor vast internet). Met uitzondering van de IP-adressen (zie artikel 127, § 3, derde lid, van de WEC).			
De nooddiensten die ter plaatse hulp bieden[31] en de beheerscentrales van de medische hulpdiensten en van de politiediensten die vanop afstand hulp bieden	Ja	Ja	Ja	Art. 107, §2 en 107, § 4, van de WEC[32]

Meer gedetailleerde informatie is terug te vinden in de fiches die op de BIPT-website worden gepubliceerd[33] (voor elke autoriteit werd een fiche opgesteld, behalve voor de nooddiensten die ter plaatse hulp bieden).

[31] Volgens artikel 107, § 1, van de WEC, betreft het de volgende diensten:
1° de medische spoeddienst;
2° de brandweerdiensten;3° de politiediensten;4° de civiele bescherming.
[32] Dit artikel verplicht de operator die een oproep doorstuurt naar een van die nooddiensten, om hem tijdens de oproep het oproepnummer van het eindapparaat, de naam van de eindgebruiker en de plaats waar de eindapparatuur zich bevindt op het ogenblik van de oproep, te leveren. Indien die nooddiensten door technische problemen die gegevens niet kunnen krijgen, kunnen ze van de operator de meest recente bewaarde gegevens ontvangen die overeenstemmen met die gegevens.
[33] https://www.bipt.be/operatoren/wettelijke-onderschepping.

Table des matières

1. Résumé

1. La ministre des Télécommunications doit faire publier au Moniteur belge une circulaire qui « *comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127* » de la loi du 13 juin 2005 relative aux communications électroniques. Cette liste se trouve en annexe. Les autorités qui se trouvent sur cette liste ont rédigé une fiche comprenant davantage d'informations. Ces fiches sont publiées sur le site Internet de l'IBPT. Le présent document comprend également des considérations générales concernant les requêtes des autorités et leur exécution par les opérateurs.

2. Objet

2. Le présent document constitue la circulaire que la ministre des Télécommunications[1] doit publier au Moniteur belge conformément à l'article 127/1, § 5, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la loi relative aux communications électroniques). Cet article a été introduit dans cette loi par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (ci-après la loi sur la conservation des données de 2022).

3. L'article 127/1, § 5, alinéa 2, de la loi relative aux communications électroniques indique que la circulaire « *comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127* » de cette même loi. Cette liste se trouve en annexe. Des informations plus détaillées se trouvent dans des fiches publiées sur le site Internet de l'IBPT[2]. Ces fiches ont été rédigées par les autorités listées en annexe du présent document.

4. La présente circulaire comprend également des considérations générales destinées à aider les opérateurs[3] et les autorités belges compétentes dans le cadre de demande de données conservées en vertu d'un des articles précités.

5. Un opérateur a demandé que la présente circulaire reprenne la liste des autorités qui peuvent adresser aux opérateurs une requête de gel de données existantes (quick freeze) ou futures (future freeze).

6. Cependant, cette forme de conservation de données (quick freeze et future freeze) n'est pas prévue par la loi relative aux communications électroniques mais par les législations des autorités demanderesses. Dès lors, la présente circulaire ne reprend ci-après et uniquement à titre d'information les autorités belges qui peuvent adresser aux opérateurs de telles requêtes, étant donné que davantage d'informations sont reprises dans les fiches publiées sur le site Internet de l'IBPT :

[1] Selon l'article 127/1, § 5, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques, il revient au ministre de publier cette circulaire dans le Moniteur belge. L'article 2, 2°, de cette même loi définit la notion de « ministre » comme « *les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi* ».
[2] https://www.ibpt.be/operateurs/interception-legale.
[3] L'article 2, 11°, de la loi relative aux communications électroniques définit un opérateur comme « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public.* »

6.1. Les autorités judiciaires sur base des articles 39ter à 39quinquies du Code d'instruction criminelle ;

6.2. Les services de renseignement et de sécurité sur base de l'article 13/6 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

6.3. La FSMA sur base de l'article 81, § 1bis et de l'article 84, § 1bis/1 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

7. En plus d'être publiée au Moniteur belge, la présente circulaire est publiée sur le site Internet de l'IBPT[4]. Les modifications au présent document ou à son annexe seront publiées de la même manière.

8. La présente circulaire est interprétative et est destinée aux opérateurs et aux autorités belges qui peuvent obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques.

3. Notions

Différents types de données

9. L'article 3, 9), du Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (ci-après le règlement relatif aux preuves électroniques en matière pénale)[5] définit les « **données relatives aux abonnés** » comme « *toutes données détenues par un fournisseur de services concernant l'abonnement à ses services, relatives à:*

a) l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis ;

b) le type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques connexes ou les interfaces utilisées ou fournies par l'abonné ou le client au moment du premier enregistrement ou de la première activation, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou autres moyens d'authentification utilisés à la place d'un mot de passe qui sont fournis par un utilisateur ou créés à la demande d'un utilisateur. »

10. Plusieurs législations européennes font référence à la notion de **données de trafic** :

10.1. L'article 2, alinéa 2, b), de la directive « vie privée et communications électroniques »[6] définit les « données relatives au trafic » comme « *b) toutes les données traitées en*

[4] https://www.ibpt.be/operateurs/interception-legale.
[5] J.O. L 191/118 du 28.07.2023.
[6] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » ;

10.2. L'article 3, 11), du règlement relatif aux preuves électroniques en matière pénale définit les « données relatives au trafic comme « *les données relatives à la fourniture d'un service proposé par un fournisseur de services qui servent à fournir des informations contextuelles ou supplémentaires sur ce service et qui sont générées ou traitées par un système d'information du fournisseur de services, tels que la source et la destination d'un message ou un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service* ».

11. L'article 9 de la directive « vie privée et communications électroniques » (transposé dans l'article 123 de la loi relative aux communications électroniques) vise le traitement par les opérateurs de « **données de localisation autres que les données relatives au trafic** ». Il s'agit de données de localisation nécessaires pour le fonctionnement du réseau mais qui ne sont pas liées à une communication de contenu.

12. L'article 2, 93°, de la loi relative aux communications électroniques définit les « **métadonnées de communications électroniques »** comme suit « *les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.* » Cette définition a été reprise du projet de règlement « vie privée et communications électroniques », qui a été proposé par la Commission européenne pour remplacer la directive vie privée et communications électroniques[7].

13. Plusieurs législations définissent la notion de **contenu** :

13.1. L'article 3, 12), du règlement relatif aux preuves électroniques en matière pénale définit les « données relatives au contenu » comme « *toutes données dans un format numérique telles que du texte, de la voix, des vidéos, des images et du son, autres que les données relatives aux abonnés ou les données relatives au trafic* » ;

13.2. L'article 2, 92°, définit le « contenu de communications électroniques » comme « *le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son* ».

14. L'article 3, 8), du règlement relatif aux preuves électroniques regroupe les différentes catégories de données sous la notion de « **preuves électroniques** »: « *les données relatives aux abonnés, les données relatives au trafic ou les données relatives au contenu stockées par un fournisseur de services ou pour le compte d'un fournisseur de services, sous une forme numérique, au moment de la réception d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR)* ».

[7] Proposal of 10.1.2017 of the European Commission for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

15. Les relations entre les différents types de données sont les suivantes.

16. Les notions de données de trafic au sens de la directive « vie privée et communications électroniques » et de métadonnées au sens de la loi relative aux communications électroniques sont similaires. Il convient cependant de noter les différences suivantes :

16.1. La notion de métadonnées exclut les données de trafic qui sont nécessaires pour la facturation (par exemple le nom et l'adresse (électronique) de l'abonné pour envoyer la facture) et qui ne répondent pas à la définition de métadonnées ;

16.2. La notion de métadonnées inclut les données de localisation autres que les données relatives au trafic, étant donné que la notion de métadonnées inclut « *les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques* ».

17. Les données de trafic ou de métadonnées ne sont pas des données du contenu de la communications électroniques.

18. Les articles 126 et 127 de la loi relative aux communications électroniques obligent les opérateurs à conserver des données, dans le but ultime d'identifier l'utilisateur final. Cependant, cela n'exclut pas que l'article 126 puisse contenir des données de trafic (ou métadonnées). Ainsi, selon l'article 126, § 1er, 15°, les opérateurs doivent conserver l'adresse IP à la source de la connexion et selon la jurisprudence de la CJUE, les adresses IP font partie des données relatives au trafic[8].

19. Le fait que les adresses IP peuvent être utiles pour identifier l'utilisateur final est reflété dans la définition de « données demandées à la seule fin d'identifier l'utilisateur » de l'article 3, 10) du règlement relatif aux preuves électroniques en matière pénale : « *les adresses IP et, si nécessaire, les ports de provenance et l'horodatage pertinents, à savoir la date et l'heure, ou les équivalents techniques de ces identifiants et les informations connexes, lorsque les services répressifs ou les autorités judiciaires les demandent à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique* ».

20. Les données que les opérateurs doivent conserver en vertu des articles 126/1 à 126/3[9] de la loi relative aux communications électroniques (conservation de données ciblée sur base géographique) sont des données de trafic (ou métadonnées).

Notion de requête

21. Le présent document utilise la notion de « requête » pour désigner la demande formelle d'une autorité envers un opérateur de lui fournir des données conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques. En pratique, la requête d'une autorité peut porter une autre dénomination (par exemple le réquisitoire ou la réquisition).

[8] C.J.U.E, arrêt *La Quadrature du Net,* 6 octobre 2020, C-511/18, C-512/18 et C- 520/18, point 152.
[9] L'article 127/1, § 5, de la loi relative aux communications électroniques, qui constitue le fondement juridique de la présente circulaire, vise les articles 126/1 et 126/3. En réalité, ce sont les articles 126/1, 126/2 et 126/3 qui sont consacrés à la conservation ciblée sur base géographique et les données à conserver dans ce cadre sont listées à l'article 126/2, § 2.

4. La compétence matérielle de l'autorité qui requiert les données

Aperçu des deux conditions reprises dans l'article 127/1 de la loi relative aux communications électroniques

22. Les paragraphes 2 à 4 de l'article 127/1 de la loi relative aux communications électroniques prévoient ce qui suit :

« *§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle :*

1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique ;

3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques ;

4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information ;

5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques ;

6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave ;

7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;

9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;

10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.

§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.

Seules les autorités visées au paragraphe 2 peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127, pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.

Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.

§ 4. Les données conservées en vertu des articles 126/1 et 126/3 le sont pour les autorités

et finalités visées au paragraphe 2, 1° à 3° et 6°.

Seules les autorités visées au paragraphe 2, 1° à 3°, 6° et 9°, peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu des articles 126/1 et 126/3, pour autant que prévu par et aux conditions fixées dans une norme législative formelle. »

23. Ces paragraphes visent l'hypothèse selon laquelle une autorité belge exige d'un opérateur qu'il lui fournisse des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques.

24. L'exposé des motifs de la loi sur la conservation des données de 2022 prévoit que l'article 127/1 de la loi relative aux communications électroniques ne s'applique pas « *aux situations dans lesquelles les données sont transmises à une autorité par l'une des parties à la communication ou demandées par une autorité à l'une des parties. Entre notamment dans cette dernière hypothèse, la situation ou une partie transmet à une autorité ses métadonnées à des fins de plainte, de règlement d'un litige ou d'une instruction d'office*[10]*.* » (page 96)

25. Cette situation est rencontrée à l'article 122, § 6, de la loi relative aux communications électroniques, qui prévoit ce qui suit : « *L'Institut, le Service de médiation pour les télécommunications, l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'Etat peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation.* »

26. Cette disposition ne constitue pas une base légale qui permet à ces différentes autorités d'exiger des données des opérateurs, conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques, mais vise la situation dans laquelle une partie à la communication (qui, le cas échant, peut être l'opérateur lui-même) transmet des données à l'autorité.

27. Par ailleurs, l'exposé des motifs de la loi sur la conservation des données de 2022 prévoit que l'article 127/1 de la loi relative aux communications électroniques ne s'applique pas non plus :« *lorsqu'un operateur transmet des données anonymes à un tiers. Les données doivent être rendues anonymes conformément aux exigences du RGPD et doivent être rendues anonymes par rapport aux personnes physiques et morales auxquelles ces données se rapportent (et pas uniquement par rapport aux personnes physiques comme c'est le cas dans le RGPD). En effet, la directive « vie privée et communications électroniques » (directive 2002/58) protège la confidentialité des données liées tant aux personnes morales qu'aux personnes physiques.* » (page 96)

28. Il ressort de l'article 127/1 qu'un opérateur ne peut pas utiliser pour ses propres besoins des données conservées en vertu des articles 126, 126/1, 126/3 ou 127, qui sont des données conservées pour les autorités. Ce principe est sans préjudice de la possibilité pour un opérateur de conserver, dans les conditions fixées par la loi (voir en particulier les articles 122 et 123 de la loi relative aux communications électroniques), des données pour ses propres besoins ou dans l'intérêt de ses clients.

29. Conformément à l'article 127/1, §§ 2 à 4, de la loi relative aux communications électroniques, un opérateur ne peut pas communiquer à un tiers des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications

[10] Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, Doc., Ch., 2021-2022, n°2572/001.

électroniques, sauf dans les hypothèses prévues dans cet article 127/1 et qui sont exposées ci-dessous.

30. Comme il ressort de l'article 127/1 de la loi relative aux communications électroniques et de l'exposé des motifs de la loi sur la conservation des données de 2022, une autorité belge qui exige d'un opérateur de lui fournir des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques doit répondre aux deux conditions cumulatives suivantes :

30.1. elle doit remplir l'une des finalités d'accès aux données visées à l'article 127/1[11], et ;

30.2. une norme législative formelle doit l'habiliter à requérir ces données à l'opérateur.

31. Ces deux conditions sont examinées plus en détail ci-dessous.

Première condition : remplir une finalité d'accès aux données reprise à l'article 127/1 de la loi relative aux communications électroniques

32. L'autorité qui exige d'un opérateur de lui fournir des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques doit remplir l'une des finalités d'accès aux données visées à l'article 127/1 de cette même loi.

33. Les finalités d'accès admises sont différentes selon que les données auxquelles l'autorité accède sont conservées en vertu :

33.1. des articles 122 et 123 de la loi relative aux communications électroniques (données conservées par les opérateurs pour leurs propres besoins ou dans l'intérêt de leurs clients), ou ;

33.2. des articles 126 et 127 de la loi relative aux communications électroniques (données (techniques) en vue d'identifier l'utilisateur final), ou ;

33.3. des articles 126/1 à 126/3 de la loi relative aux communications électroniques (métadonnées conservées dans le cadre de la conservation ciblée sur base géographique).

34. Le tableau ci-dessous reprend la liste exhaustive des finalités d'accès admises selon le type de données conservées :

Ensemble des finalités d'accès visées dans l'article 127/1, § 2	Finalités d'accès admises selon les différents types de données conservées

[11] La notion d'accès aux données se retrouve dans la jurisprudence de la CJUE et permet de simplifier le texte mais, en pratique, les opérateurs fournissent aux autorités les données demandées.

	Données art. 122 et 123[12]	Données art. 126 et 127[13]	Données art. 126/1 à 126/3[14]
1° les services de renseignement et de sécurité afin d'accomplir les missions en vertu de la loi des services de renseignement et de sécurité[15]	Oui	Oui	Oui
2° la prévention de menaces graves pour la sécurité publique	Oui	Oui	Oui
3° la sauvegarde des intérêts vitaux de personnes physiques	Oui	Oui	Oui
4° l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information	Oui	Oui	Non
5° la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques	Oui	Oui	Non
6° la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave	Oui	Oui	Oui
7° préserver un intérêt économique ou financier important de l'UE ou de la Belgique	Oui	Oui	Non
8° la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave	Oui	Oui	Non
9° l'IBPT dans le cadre du contrôle de la loi relative aux communications électroniques et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle	Oui	Oui	Oui
10° la recherche scientifique ou historique ou fins statistiques	Oui	Oui (sauf adresse IP)	Non

35. A titre d'exemple, « l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information » (finalité d'accès reprise à l'article 127/1, § 2, 4°, de la loi relative aux communications électroniques) permet aux autorités compétentes en la matière de remplir la première condition de l'article 127/1 (finalité d'accès, cf. supra) pour ce qui concerne les données conservées par les opérateurs conformément aux articles 122, 123, 126 et 127 mais pas pour les données conservées par

[12] Voir article 127/1, § 2.
[13] Voir article 127/1, § 3. L'article 127/1, § 3, alinéa 3 précise que « *Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.* »
[14] Voir article 127/1, § 4.
[15] Loi organique des services de renseignement et de sécurité du 30 novembre 1998.

ces mêmes opérateurs conformément aux articles 126/1 à 126/3 (données conservées sur base géographique).

36. L'article 127/1, § 1er, de la loi relative aux communications électroniques indique ce qui suit :

« […], *la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux :*

1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle ;

2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique ;

3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles. »

Deuxième condition : la norme législative formelle

37. L'autorité qui exige d'un opérateur qu'il lui fournisse des données personnelles conservées en vertu des articles 122, 123, 126, 126/1 à 126/3 ou 127 de la loi relative aux communications électroniques doit également disposer d'une norme législative formelle qui l'habilite à requérir ces données de l'opérateur. A titre d'exemple, les autorités qui sont compétentes pour « l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information » (finalité d'accès reprise à l'article 127/1, § 2, 4°, de la loi relative aux communications électroniques) ne pourront en pratique accéder aux données conservées par les opérateurs conformément aux articles 122, 123, 126 et 127, que pour autant que la loi organique de ces autorités le prévoie expressément et selon les conditions fixées par cette loi.

38. Selon l'exposé des motifs de la loi sur la conservation des données de 2022, la norme législative formelle « *doit avoir au moins le niveau d'une loi : loi fédérale, décret, ordonnance, règlement européen, etc.* » (page 96)

39. Cette norme législative formelle doit préciser :

> « *— la ou les catégories d'entreprises auxquelles l'autorité peut demander des données ;*
> *— les catégories de données qui peuvent être demandées ;*
> *— les finalités poursuivies ;*
> *— les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.* »
> (art. 127/1, § 5, de la loi relative aux communications électroniques).

40. Cette disposition fait l'objet des explications suivantes dans l'exposé des motifs de la loi sur la conservation des données de 2022 (pages 115 et 116) :

« *Afin d'éviter toute interprétation de la législation organique ou sectorielle sur laquelle une autorité se base pour obtenir les données de l'opérateur, il est essentiel que cette législation*

prévoie le pouvoir de l'autorité d'obtenir les données de l'opérateur (ou une expression équivalente, cette notion pouvant être plus large que la notion d'opérateur au sens de la loi télécom) et ne se contente pas de prévoir un pouvoir d'obtenir des données de toute personne. Il est aussi essentiel que cette législation prévoie que l'autorité peut obtenir des données d'identification ou des métadonnées (ou toute expression qui vise à préciser les données à obtenir de l'opérateur) et ne se contente pas de prévoir que l'autorité peut demander toute information utile […] Ne peuvent pas être reprises sur cette circulaire des autorités qui seraient simplement légalement habilitées à demander à des acteurs économiques toute donnée utile. »

41. Par ailleurs, dans son arrêt La Quadrature du Net du 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), la CJUE admet que les États membres imposent aux opérateurs certaines mesures de conservation de données « *dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.* » (dispositif de l'arrêt)

42. C'est la norme législative formelle qui doit contenir ces conditions matérielles et procédurales et les garanties contre les abus.

Liste des autorités qui déclarent répondre aux deux conditions

43. L'annexe à la présente circulaire comprend une liste d'autorités qui déclarent répondre aux deux conditions susmentionnées.

44. L'objectif poursuivi est que cette liste soit aussi exhaustive que possible. Cependant, il convient de noter que celle-ci a été établie sur la base des informations communiquées par les autorités concernées à l'IBPT et à la ministre des Télécommunications. Son caractère exhaustif ne peut donc être garanti.

45. Si une autorité demande des données à un opérateur, conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques, sans être reprise sur cette liste, elle devra indiquer à l'opérateur qu'elle répond bien aux deux conditions susmentionnées : répondre à une des finalités d'accès prévues par l'article 127/1, §§ 2 à 4, de la loi relative aux communications électroniques et disposer d'une norme législative formelle qui répond aux exigences du paragraphe 5, alinéa 1er, de ce même article. Le simple fait qu'une autorité ne soit pas reprise dans cette liste ne justifie toutefois pas que l'opérateur refuse de donner suite à la demande qui lui est adressée par cette autorité.

46. Si l'une de ces conditions n'est pas remplie, l'opérateur devra refuser d'exécuter la requête. Si les deux conditions sont remplies, l'autorité devra être reprise sur la liste en annexe. Afin que cette liste puisse être mise à jour de manière à refléter au mieux la réalité, il est demandé ce qui suit :

46.1. toute autorité qui ne figure pas sur la liste mais qui estimerait disposer des habilitations légales lui permettant d'y être reprise est priée de le porter à la connaissance de l'IBPT et du cabinet du ou de la ministre des Télécommunications ;

46.2. de même, les autorités concernées sont également priées de leur notifier toute modification de leur législation qui nécessiterait une adaptation de cette liste.

47. Enfin, il convient de rappeler la nature purement interprétative de la présente circulaire, qui n'a pas force de loi, et est formulée sous réserve de l'interprétation des cours et tribunaux.

5. La compétence territoriale de l'autorité qui requiert les données

48. Il résulte de l'arrêt du 1er décembre 2015 (P. 13.2082.N/1, YAHOO! Inc.) de la Cour de cassation de Belgique qu'un opérateur est soumis à la législation belge du seul fait de sa participation active à la vie économique en Belgique et doit donc faire droit à une demande de données du procureur du Roi conformément à l'article 46bis du Code d'instruction criminelle :

« *2. L'article 46bis Code d'instruction criminelle dispose :*

- au paragraphe 1er, alinea 1er, qu'en recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, requérir le concours de l'opérateur d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique afin d'obtenir les données prévues par cette disposition ;

- au paragraphe 2, alinéa 1er, que chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe 1er, les fournisse au procureur du Roi.

3. Au paragraphe 2, alinéa 4, cette disposition énonce aussi que le refus de communiquer les données visées est puni d'une amende. Cette sanction pénale vise à imposer l'obligation de concours incombant aux opérateurs et fournisseurs visés et confère, dans cette mesure, à l'article 46bis, § 2, du Code d'instruction criminelle le caractère d'une mesure coercitive.

4. En règle générale, un État ne peut prendre des mesures coercitives que sur son propre territoire afin d'imposer le respect de ses lois et, s'il prend une telle mesure sur le territoire d'un autre État, il s'approprie un pouvoir extraterritorial qui méconnaît la souveraineté de cet État.

5. Un État prend une mesure coercitive sur son propre territoire lorsqu'il existe un lien territorial suffisant entre cette mesure et ce territoire. Le lien qui est, à tout le moins, requis, est notamment déterminé par la nature et la portée de la mesure coercitive.

6. La sanction pénale prévue à l'article 46bis, § 2, alinéa 4, du Code d'instruction criminelle vise uniquement à imposer aux opérateurs et fournisseurs actifs depuis la Belgique une mesure ayant pour objectif d'obtenir de simples éléments d'identification ensuite d'une infraction dont l'enquête relève de la compétence des juridictions répressives belges. Cette mesure ne requiert pas la présence à l'étranger des fonctionnaires de police ou magistrats belges, ni de personnes agissant pour leur compte. Cette mesure ne requiert pas davantage la commission d'un quelconque acte matériel à l'étranger. Elle concerne, par conséquent, une mesure coercitive dont la portée est limitée et dont l'exécution ne requiert aucune intervention en dehors du territoire belge.

7. L'article 3 du Code pénal dispose que l'infraction commise sur le territoire du royaume, par des Belges ou par des étrangers, est punie conformément aux dispositions des lois belges. L'infraction prévue à l'article 46bis, § 2, alinéa 4, du Code d'instruction criminelle est commise en un lieu où les données requises doivent être reçues. Par conséquent, l'opérateur ou le fournisseur qui refuse de communiquer ces données est passible d'une peine en Belgique, quel que soit le lieu où il est établi.

8. Il ressort de ce qui précède, d'une part, que la mesure consistant en l'obligation de fournir les données visées en l'espèce est prise sur le territoire belge à l'égard de chaque opérateur ou fournisseur qui oriente activement ses activités économiques vers des consommateurs en Belgique et, d'autre part, que la juridiction belge qui condamne un opérateur ou fournisseur établi à l'étranger en raison de l'inobservation de cette obligation et impose ainsi le respect d'une mesure prise en Belgique, n'exerce pas de pouvoir de juridiction extraterritorial. Dans la mesure où il est déduit d'une autre prémisse juridique, le moyen manque en droit.

9. Les juges d'appel, adoptant les motifs du jugement entrepris et par des motifs propres, ont considéré notamment que la demanderesse, en tant que fournisseur d'un service de messagerie électronique gratuit, est présente sur le territoire de la Belgique et se soumet volontairement à la loi belge parce qu'elle participe activement à la vie économique en Belgique notamment par l'usage du nom de domaine « www.yahoo.be », l'usage de la langue locale, par la publicité faite en fonction de la localisation des utilisateurs de ses services et par son accessibilité en Belgique pour ces utilisateurs via notamment une boîte de réclamations et une rubrique FAQ. En adoptant les motifs du jugement entrepris (points 4.2. et 4.4.), les juges d'appel ont aussi considéré que :

- le procureur du Roi ne demande rien, aux États-Unis, à un ressortissant de ce pays mais, substantiellement, demande quelque chose en Belgique à un ressortissant de ce pays prestataire de services en Belgique ; ».

49. Ce même raisonnement a été répété dans l'arrêt du 19 février 2019 (P.17.1229.N/1, Skype communications) de la Cour de cassation de Belgique mais cette fois pour une demande de fournir le contenu d'une communication électronique à un juge d'instruction :

« *8. L'article 88bis du Code d'instruction criminelle, tel qu'applicable en l'espèce, dispose :*
« § 1er. Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication directement ou par l'intermédiaire d'un service de police désigné par le Roi :

1° au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés ;
2° à la localisation de l'origine ou de la destination de télécommunications.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi.

Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement.
[…]
§ 2. Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication communique les informations qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les télécommunications.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les télécommunications, est punie d'une amende de vingt-six euros à dix mille euros. »

L'article 90quater, § 2, du Code d'instruction criminelle, tel qu'applicable en l'espèce, dispose :

« Si la mesure comporte une opération sur un réseau de communication, l'opérateur de ce réseau, ou le fournisseur du service de télécommunication, est tenu de prêter son concours technique, quand le juge d'instruction le requiert directement ou par l'intermédiaire d'un service de police désigné par le Roi.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les télécommunications, est punie d'une amende de vingt-six euros à dix mille euros. »

Ces dispositions permettent au juge d'instruction belge, dans le cadre de son instruction, de demander à chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de messagerie électronique dont l'activité économique s'adresse activement aux consommateurs en Belgique, de communiquer les informations ou de fournir l'assistance technique visées en l'espèce, indépendamment du lieu où cet opérateur ou ce fournisseur est établi ou du lieu où se situe l'infrastructure requise pour donner suite à la demande du juge d'instruction.

En effet, d'une part un tel opérateur ou fournisseur est soumis à la législation belge du seul fait de sa participation active à la vie économique en Belgique.

D'autre part, l'obligation de coopérer ainsi visée ne requiert pas l'intervention des autorités judiciaires belges à l'étranger. Par conséquent, le juge d'instruction n'est pas tenu d'adresser sa demande d'entraide judiciaire à l'État où le siège ou l'infrastructure de cet opérateur ou de ce fournisseur se situent et n'est pas davantage lié par la législation de ce pays. »

6. Les mentions minimales de la requête adressée à l'opérateur

50. L'article 127/1, § 6, de la loi relative aux communications électroniques prévoit ce qui suit :

« *Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes :*
1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service ;

2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central ;
3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité ;
4° le délai de réponse souhaité. »

51. L'article 127/1, § 6, 3°, précité prévoit que la requête doit comprendre « *la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité ».* Ce service central est en pratique le « NTSU », à savoir le *National Technical & Tactical Support Unit* des unités spéciales de la police fédérale. En pratique, lorsque la demande de données est envoyée à l'opérateur par le biais du NTSU, l'autorité demanderesse introduit la demande de données dans la plateforme d'échange TANK du NTSU[16]. Dans ce cas, la requête (qui contient la base légale) doit aussi être introduite dans cette plateforme.

52. Un opérateur doit refuser une requête écrite qui n'est pas signée. Si la signature est électronique, elle doit répondre aux exigences légales en la matière. Une signature en dessous d'un email ne répond pas à ces exigences.

7. Le contrôle interne ou externe de la requête

53. L'article 4 du règlement relatif aux preuves électroniques en matière pénale fait la distinction entre :

- « *1. Une injonction européenne de production visant à obtenir des données relatives aux abonnés ou visant à obtenir des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10)*[17] », et ;

- « *2. Une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10) […]* ».

54. On retrouve une distinction similaire en droit belge. Ainsi, le Code d'instruction criminelle prévoit ce qui suit[18] :

« *46bis. § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues*

[16] Il s'agit d'une plateforme gérée par le NTSU, qui permet d'envoyer aux opérateurs certaines demandes de données des autorités judiciaires et des services de renseignement et de sécurité et de recevoir la réponse des opérateurs.
[17] L'article 3, point 10), de ce règlement définit les « données demandées à la seule fin d'identifier l'utilisateur » comme suit : « les adresses IP et, si nécessaire, les ports de provenance et l'horodatage pertinents, à savoir la date et l'heure, ou les équivalents techniques de ces identifiants et les informations connexes, lorsque les services répressifs ou les autorités judiciaires les demandent à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique ».
[18] Il en va de même pour les articles 81, § 1er, alinéa 1er, et 84, § 1er, alinéa 1er, de la loi sur la surveillance financière (loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers), dont la terminologie utilisée est presque identique à celle respectivement des articles 46bis et 88 bis du Code d'instruction criminelle. Voir également, l'article 2, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé ;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. »
(nous soulignons)

« Art. 88bis. § 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques. »
(nous soulignons)

55. Cette distinction est aussi reflétée pour ce qui concerne le contrôle de la requête, comme expliqué ci-dessous.

56. Comme exigé par la jurisprudence de la CJUE[19], en cas de demande de trafic, à l'exception de données demandées à la seule fin d'identifier l'utilisateur et sauf cas d'urgence, la requête de l'autorité doit faire l'objet d'un contrôle préalable par une autorité administrative indépendante (par exemple l'Autorité de protection des données) ou une juridiction (par exemple un juge d'instruction). En cas d'urgence, le contrôle doit intervenir dans un bref délai. Ce contrôle (préalable ou a posteriori) est un contrôle externe, étant donné que le contrôle est effectué par une autorité distincte de la personne ou de l'autorité demanderesse.

57. En cas de demande de données relatives aux abonnés ou visant à obtenir des données à la seule fin d'identifier l'utilisateur, ce contrôle externe n'est pas requis mais un contrôle interne (contrôle au sein de l'autorité demanderesse) est nécessaire. Ce contrôle interne comprend par exemple une vérification du respect des formalités (par exemple la présence des signatures requises, la référence à la base légale), de la nécessité et de la proportionnalité de la demande. Il est effectué par exemple par le procureur du Roi, par le préposé à la protection des données à caractère personnel (DPO ou Data protection officer) de l'autorité demanderesse, le supérieur hiérarchique ou l'officier de police judiciaire désigné spécialement à cet effet pour ce qui concerne la loi sur le statut de l'IBPT[20].

58. C'est la législation organique de l'autorité demanderesse qui détermine quel contrôle doit être effectué (interne ou externe), par qui et en quoi il consiste. Les contrôles interne et externe font référence à un contrôle par une autorité et non au contrôle effectué par l'opérateur.

59. Cette distinction entre contrôle externe et contrôle interne découle de l'arrêt « loi carte prépayée » de la Cour constitutionnelle (arrêt n° 158/2021 du 18 novembre 2021) :

« B.16.8.6. À cet égard, les parties requérantes renvoient à l'arrêt de la grande chambre de la Cour de justice du 2 mars 2021 en cause Prokuratuur (C-746/18, points 50 à 56), dans

[19] Arrêt Digital Rights du 8 avril 2014 (C-293/12), arrêt Tele 2 du 21 décembre 2016 (C-203/15), arrêt La Quadrature du Net du 6 octobre 2020 (C-511/18) et arrêt Prokuratuur du 2 mars 2021 (C-746/18).
[20] Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

lequel la Cour de justice exige, selon elles, qu'une autorité administrative indépendante ou un juge contrôle au préalable chaque demande d'accès au regard des droits fondamentaux et règles nationales applicables et dans lequel elle précise, selon les parties requérantes, que le ministère public, qui dirige la procédure d'enquête et exerce le cas échéant l'action publique, ne dispose pas de l'indépendance requise pour pouvoir effectuer ce contrôle.

Toutefois, cet arrêt portait sur une demande du ministère public d'obtenir un accès à des données relatives au trafic et à des données de localisation. Comme il est dit en B.14.3, la Cour de justice et la Cour européenne des droits de l'homme n'exigent en revanche pas de contrôle judiciaire ou administratif préalable pour une demande d'accès à des données d'identification. En conséquence, le droit au respect de la vie privée ne s'oppose pas à une demande d'accès à de telles données qui émane du ministère public. » (nous soulignons)

8. Demande adressée à la cellule de coordination de l'opérateur

60. Il résulte de l'article 127/3, § 1er, alinéa 3, de la loi relative aux communications électroniques qu'une autorité doit s'adresser à la Cellule de coordination de l'opérateur pour obtenir des données conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques .

61. En vertu du même article, chaque opérateur doit disposer d'une telle cellule.

62. Une autorité belge qui ne disposerait pas encore des coordonnées de la permanence de la cellule de coordination des opérateurs peut s'adresser à l'IBPT pour obtenir l'accès à ces coordonnées.

63. Si une requête vise un opérateur bien précis (et non les opérateurs de manière générale) et qu'il apparait qu'elle aurait dû être adressée à un autre opérateur (par exemple car c'est cet autre opérateur qui dispose des informations concernant le numéro de téléphone visé dans la requête), l'autorité devra adresser une nouvelle requête à cet opérateur.

9. Qu'est-ce que l'opérateur peut/doit contrôler et dans quels cas peut-il/doit-il refuser une requête?

64. L'opérateur doit contrôler que la requête provient bien de l'autorité qui prétend s'adresser à elle (et non d'une personne qui se fait passer pour cette autorité), sauf si la requête a été introduite dans la plateforme d'échange « TANK » du NTSU. En effet, dans ce cas, ce contrôle est déjà effectué grâce à l'implémentation technique et aux règles fonctionnelles de cette plateforme. L'opérateur doit refuser d'exécuter la requête de l'autorité si la mention minimale (voir titre 4 ci-dessus) suivante n'est pas reprise sur cette requête : « *1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service ».*

65. L'opérateur peut déterminer si la requête a fait l'objet d'un contrôle interne ou externe en examinant cette dernière.

66. Lorsqu'il ressort de la requête qu'elle a fait l'objet d'un contrôle externe (contrôle par une juridiction ou une autorité administrative indépendante), l'opérateur ne doit pas réaliser de contrôle complémentaire. Ceci vaut également lorsque ce contrôle est effectué après l'envoi de la requête à l'opérateur, en raison de l'urgence.

67. Lorsqu'il ressort de la requête qu'elle a fait l'objet d'un contrôle interne, il est attendu de l'opérateur qu'il procède à un contrôle de cette dernière. Lorsque c'est possible, ce contrôle est effectué avant de répondre à la requête. L'opérateur doit s'assurer que la base légale de la requête est suffisante pour requérir les données. Ainsi, l'exposé des motifs de la loi sur la conservation des données de 2022 (voir pages 116 et 117) indique ce qui suit : « *Avant de donner suite à une demande de données qui fait l'objet d'un contrôle interne, il revient à l'opérateur de vérifier l'existence de la base légale nécessaire pour requérir les données.* »

68. Un opérateur doit donc refuser de faire suite à une requête d'une autorité si elle ne repose pas sur une base légale suffisante (voir ci-dessus « 4. La compétence matérielle de l'autorité qui requiert les données » et les deux conditions à respecter). En pratique, l'opérateur pourra d'abord contrôler que la base légale de la requête est bien reprise dans l'annexe au présent document. Si c'est le cas, la base légale est en principe suffisante. Si cela n'est pas le cas, il devra examiner cette base légale plus en détail.

69. Un opérateur doit refuser d'exécuter la requête de l'autorité s'il n'apparaît pas que le contrôle interne ou externe de la requête a bien été effectué (contrôle préalable) ou sera effectué (contrôle a posteriori en cas d'urgence).

70. Ce contrôle ressort de la requête, par exemple, si elle indique qu'il a été effectué ou qu'il sera effectué (urgence). En d'autres termes, l'opérateur est autorisé à se fier à la déclaration dans la requête. Lorsque ce contrôle ne ressort pas de la requête et que l'opérateur le signale à l'autorité demanderesse, cette dernière peut informer l'opérateur que ce contrôle a bien été effectué (contrôle préalable) ou sera effectué (contrôle a posteriori en cas d'urgence).

71. En revanche, l'opérateur ne peut pas refuser d'exécuter la requête, au motif qu'il n'a pas pu prendre connaissance des documents échangés entre les différentes personnes ou autorités dans le cadre du contrôle interne ou externe.

72. Lorsqu'un opérateur refuse de faire suite à une requête, il doit en informer l'autorité demanderesse.

73. Comme expliqué dans l'exposé des motifs de la loi sur la conservation des données de 2022 (voir pages 116 et 117), *« que le contrôle soit interne ou externe, il ne revient pas à l'opérateur de juger de la proportionnalité des demandes de données de cette autorité ni de vérifier si la demande est suffisamment motivée.* »

74. Cependant, sans que cela ne constitue un argument pouvant être utilisé par l'opérateur pour refuser de se conformer à la requête, rien n'empêche l'opérateur de faire savoir à l'autorité demanderesse que cette requête lui semble disproportionnée, car elle nécessite une charge énorme de travail, afin de cette autorité puisse prendre conscience de l'ampleur de la requête et mieux évaluer la proportionnalité de cette dernière.

10. Les solutions en cas de différend entre l'opérateur et une autorité belge concernant une demande de données

75. L'IBPT n'est pas habilité à trancher un conflit entre un opérateur et une autorité. Le rôle de l'IBPT se limite :

75.1. à indiquer à un opérateur ou à une autorité, qui l'interroge sur ce sujet, la manière dont il entend appliquer la loi ;

75.2. à contrôler l'opérateur par rapport à certaines dispositions (par exemple la loi relative aux communications électroniques et ses arrêtés d'exécution mais pas les lois organiques d'autres autorités que l'IBPT ou le Service de médiation pour les télécommunications)[21].

76. En cas de conflit persistant, il reviendra aux cours et tribunaux de trancher le conflit.

77. Un opérateur ne peut être sanctionné pour ne pas fournir à une autorité une donnée dont il ne dispose pas (par exemple si l'opérateur ne dispose pas d'une donnée d'identification mais uniquement de données de souscription au service). Cependant, l'opérateur peut être sanctionné s'il ne respecte pas l'article 127 de la loi relative aux communications électroniques concernant l'identification de ses abonnés ou s'il ne conserve pas les données comme prévu aux articles 122, 123 et 126 à 126/3.

11. Annexe

78. Liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques.

Donné le

La Ministre des Télécommunications

P. DE SUTTER

[21] La liste des dispositions contrôlées par l'IBPT figure à l'article 14, § 1er, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

Annexe à la circulaire : liste des autorités belges qui sont légalement habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123[22], 126, 127[23], 126/1 et 126/3[24] de la loi du 13 juin 2005 relative aux communications électroniques (LCE)

Autorités	Données conservées sur base des art. 122 et 123 de la LCE	Données conservées sur base des art. 126 et 127 de la LCE	Données conservées sur base des art. 126/1 à 126/3 de la LCE	Base légale
Les autorités judiciaires (procureur du Roi, juge d'instruction, procureur européen et procureurs européens délégués)	Oui	Oui	Oui, mais uniquement pour les faits visés à l'article 127/1, § 1er, 1°, de LCE (criminalité grave)[25]	Art. 46bis, 88bis, 464/13 et 464/25 du Code d'instruction criminelle. Voir aussi art. 47quaterdecies du même Code en ce qui concerne les procureurs européens.
Cellule personnes disparues de la police fédérale	Oui	Oui	Oui	Art. 42, § 2, de la loi du 5 août 1992 sur la fonction de police
Les services de renseignement et de sécurité	Oui	Oui	Oui	Art. 16/2, 18/7, 18/8 et 18/17 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998
L'Autorité belge de la Concurrence (ABC)	Oui	Oui	Non	Art. IV.40, § 1er/1, du Code de droit économique
L'Autorité des services et marchés financiers (FSMA)	Oui	Oui	Oui, mais uniquement pour les faits visés à l'article 127/1, § 1er, de la LCE dont, entre autres, ceux visés à l'article	Art. 81, 82, 2° et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

[22] Données conservées sur base des articles 122 et 123 : données de trafic et de localisation conservées par les opérateurs pour leurs propres besoins ou dans l'intérêt de leurs clients.
[23] Données conservées sur base des articles 126 et 127 : données (en ce compris les adresses IP) en vue de l'identification de l'utilisateur final.
[24] Données conservées sur base des articles 126/1 à 126/3 : métadonnées conservées dans le cadre de la conservation ciblée sur base géographique.
[25] Il s'agit des faits pour lesquels il existe des indices sérieux qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle. Au 4/09/2023, cette peine minimale est un an d'emprisonnement.

Autorités	Données conservées sur base des art. 122 et 123 de la LCE	Données conservées sur base des art. 126 et 127 de la LCE	Données conservées sur base des art. 126/1 à 126/3 de la LCE	Base légale
			127/1, § 1er, 3°[26] (criminalité grave)	
Le service d'Inspection de la Direction-générale Animaux, Végétaux et Alimentation du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement	Oui, uniquement à des fins d'identification	Oui	Non	Art. 11, § 1, de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits
Le service de médiation pour les télécommunications	Oui, uniquement à des fins d'identification	Oui	Non	Art. 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques
Les services d'inspection suivants du SPF Economie : -DG de l'Energie (E2) ; -DG de la Qualité et de la Sécurité (E6) ; -DG de l'Inspection économique (E7)	Oui Pour obtenir des données de trafic, de localisation et les adresses IP : uniquement pour les faits visés à l'article 127/1, § 1er, 2°, de la LCE (criminalité grave)[27]	Oui Pour obtenir des adresses IP : uniquement pour les faits visés à l'article 127/1, § 1er, 2°, de la LCE (criminalité grave)[28]	Oui, mais uniquement pour les faits visés à l'art. 127/1, § 1er, 2°, de la LCE (criminalité grave)[29]	Art. XV.3, 5°/1, du Code de droit économique
Les officiers de police judiciaire (OPJ) de l'Institut belge des services postaux et	Oui	Oui	Oui, mais uniquement dans le cadre du contrôle du respect par l'opérateur de la LCE	Art. 25/1 de la loi du 17 janvier 2003 relative au statut du régulateur des

[26] Il s'agit des faits qui pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles.
[27] Il s'agit des faits pour lesquels il existe des indices sérieux qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique.
[28] Idem.
[29] Idem.

Autorités	Données conservées sur base des art. 122 et 123 de la LCE	Données conservées sur base des art. 126 et 127 de la LCE	Données conservées sur base des art. 126/1 à 126/3 de la LCE	Base légale
des télécommunications (IBPT)				secteurs des postes et des télécommunications belges
L'IBPT agissant dans le cadre d'une procédure administrative	Oui	Oui	Oui, mais uniquement dans le cadre du contrôle du respect par l'opérateur de la LCE	Art. 15 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges
Le Centre pour la Cybersécurité Belgique (CCB)[30]	Oui	Oui	Oui	Art. 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique
La Direction générale Statistique – Statistics Belgium du SPF Economie, PME, Classes moyennes et Energie	Données relatives à l'accès, l'utilisation et l'accessibilité financière des services de communications électroniques. Données : - Identité de la personne qui a conclu le contrat (nom et adresse ou numéro registre national) ; - Identité de l'entreprise qui a conclu le contrat (nom et adresse ou numéro BCE ou numéro de TVA) ; - Identité de la personne ou de l'entreprise à laquelle la facture est adressée ; - Le montant de la facture ; - La période à laquelle se rapportent les services facturés ; - La ventilation du coût par service (internet fixe, internet mobile, téléphonie fixe, téléphonie mobile et télévision numérique) ;		Non	Art. 24*sexies* de la loi du 4 juillet 1962 relative à la statistique publique

[30] En tant que CSIRT national au sens de l'article 7, § 2, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Autorités	Données conservées sur base des art. 122 et 123 de la LCE	Données conservées sur base des art. 126 et 127 de la LCE	Données conservées sur base des art. 126/1 à 126/3 de la LCE	Base légale
	- Informations sur le type de connexion en termes de vitesse potentielle (pour l'internet fixe uniquement). A l'exclusion des adresses IP (voir article 127, § 3, alinéa 3, de la LCE).			
Les services d'urgence offrant de l'aide sur place[31] et les centrales de gestion du service médical d'urgence et des services de police offrant de l'aide à distance	Oui	Oui	Oui	Art. 107, §2 et 107, § 4, de la LCE[32]

Des informations plus détaillées se trouvent dans des fiches publiées sur le site internet de l'IBPT[33] (une fiche a été établie pour chaque autorité à l'exception des services d'urgence offrant de l'aide sur place).

[31] Selon l'article 107, § 1er, de la LCE, il s'agit des services suivants :
1° le service médical d'urgence ;
2° les services d'incendie ;
3° les services de police ;
4° la protection civile.

[32] Cet article oblige l'opérateur qui achemine un appel vers un de ces services d'urgence à lui fournir, lors de l'appel, le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel. Lorsqu'en raison de problème technique, ces services d'urgence ne peuvent obtenir ces données, ils pourront obtenir de l'opérateur les données conservées les plus récentes qui correspondent à ces données.

[33] https://www.ibpt.be/operateurs/interception-legale.