



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 32/2022 van 16 februari 2022

Betreft: Verzoeken om advies over de artikelen 7, 25, 1° en 47 van het ontwerp van wet houdende diverse bepalingen inzake Economie (CO-A-2021-280, CO-A-2021-281 en CO-A-2021-283)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna 'de Autoriteit'),

Aanwezig: De heren Yves-Alexandre de Montjoye en Bart Preneel;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, en met name de artikelen 23 en 26 (hierna 'WOG');

Gelet op verordening (EU) nr. 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna 'AVG');

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

Gelet op de op 23 december 2021 ontvangen adviesaanvragen van de vice-eersteminister en minister van Economie en Werk, Pierre-Yves Dermagne;

Gelet op de op 21 en 24 januari 2022 ontvangen aanvullende inlichtingen;

Gelet op het verband tussen deze drie adviesaanvragen;

brengt het volgende advies uit op 16 februari 2022:

I. ONDERWERP EN ACHTERGROND VAN DE ADVIESAANVRAAG

1. De vice-eersteminister en minister van Economie en Werk heeft de Autoriteit om advies verzocht over de artikelen 7, 25, 1° en 47 van het ontwerp van wet houdende diverse bepalingen inzake Economie (hierna 'het ontwerp' of 'het wetsontwerp').
2. De bepalingen van het ontwerp **vinden hun oorsprong in het nieuwe artikel 127/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie** (hierna 'de Telecomwet'), zoals dat zal worden ingevoegd bij het herziene 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 (hierna 'het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens'). Het nieuwe artikel 127/1 van de Telecomwet bepaalt immers de categorieën van autoriteiten¹ die bij een operator gegevens mogen opvragen die krachtens de nieuwe artikelen 122, 123, 126 en 127 van de Telecomwet worden bewaard, waarbij wordt vereist dat een andere formele wetgevende norm in die toegang voorziet en de voorwaarden bepaalt waaronder die toegang kan plaatsvinden.
3. De **drie ontwerpbe­palingen** hebben dus tot doel **de voorwaarden te regelen waaronder de Belgische mededingingsautoriteit** (hierna 'de BMA'), de **ambtenaren van de economische inspectie** (hierna 'de EI') en **het Nationaal Instituut voor de Statistiek** (hierna 'het NIS') toegang zullen kunnen krijgen tot de verkeers-, lokalisatie- of identificatiegegevens die door de telecomoperatoren worden bewaard ter uitvoering van de nieuwe artikelen 122 en volgende van de Telecomwet, zoals die zullen worden gewijzigd na de aanneming van het wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens.

II. BEHANDELING VAN DE ADVIESAANVRAAG

A. Inleidende opmerkingen

4. De mededeling van verkeers- en lokalisatiegegevens aan bepaalde autoriteiten is onder meer geregeld door 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

¹ De autoriteiten worden geïdentificeerd aan de hand van de doeleinden die zij nastreven.

elektronische communicatie (hierna 'de e-Privacyrichtlijn'), die de AVG verduidelijkt en aanvult met betrekking tot de verwerking van persoonsgegevens in de sector van de elektronische communicatie².

5. Ter herinnering: **deze richtlijn verbiedt** in beginsel³ **de bewaring en, a fortiori, de mededeling van verkeers- en lokalisatiegegevens**⁴. Krachtens artikel 15.1 van de e-Privacyrichtlijn **kunnen de lidstaten echter wetgevingsmaatregelen goedkeuren om telecomoperatoren te verplichten** verkeers- en lokalisatiegegevens **te bewaren en aan de autoriteiten mee te delen**, indien dat in een democratische samenleving **noodzakelijk, redelijk en proportioneel is om een van de legitieme doelstellingen na te streven** die in artikel 15.1 van de e-Privacyrichtlijn zijn vastgelegd⁵. Het Hof van Justitie van de Europese Unie (hierna: 'HvJEU') heeft in verschillende arresten⁶ verduidelijkt aan welke voorwaarden dergelijke wetgevingsmaatregelen moeten voldoen om naar Europees recht toelaatbaar te zijn.
6. Ten eerste heeft het HvJEU er herhaaldelijk op gewezen dat **de toegang voor overheidsinstanties tot de door de telecomoperatoren bewaarde verkeers- en lokalisatiegegevens onderworpen is aan de voorwaarde dat deze gegevens zijn bewaard op een wijze die in overeenstemming is met de e-Privacyrichtlijn**, zoals die wordt geïnterpreteerd door het HvJEU⁷. Met andere woorden, alleen indien de bewaring van verkeers- en lokalisatiegegevens in overeenstemming met de e-Privacyrichtlijn heeft plaatsgevonden, is het mogelijk te bepalen dat toegang tot deze gegevens kan worden verleend aan overheidsinstanties.
7. **De auteur van het ontwerp moet zich er dus van vergewissen dat de nieuwe bepalingen van de Telecomwet**, die bepalen onder welke voorwaarden de operatoren verkeers- en lokalisatiegegevens moeten (of mogen) bewaren, **in overeenstemming zijn met de eisen die de Europese wetgeving stelt**. In dit verband verwijst de Autoriteit **naar haar advies nr. 108/2021** van 28 juni 2021, waarin zij tal van, soms zeer fundamentele, opmerkingen heeft geformuleerd over het voorontwerp van wet betreffende het verzamelen en bewaren van telecomgegevens. **Zij dringt**

² Ter herinnering, deze richtlijn heeft tot doel de gebruikers van elektronische-communicatiediensten te beschermen tegen de gevaren voor hun persoonsgegevens en hun privacy die voortvloeien uit de nieuwe technologieën.

³ In de artikelen 6 en 9 wordt bepaald dat aanbieders van openbare elektronische-communicatienetwerken en -diensten in bepaalde omstandigheden en met toestemming van de gebruikers of abonnees verkeers- en lokalisatiegegevens mogen verwerken en bewaren.

⁴ Zie de artikelen 5 en 9 van de e-Privacyrichtlijn.

⁵ Het gaat om de volgende motieven: *"ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG."* De Autoriteit merkt op dat het vaste rechtspraak van het HvJEU is dat de verwijzing naar artikel 13 van richtlijn 95/46 aldus moet worden gelezen dat de lidstaten maatregelen mogen nemen ter beperking van de geheimhoudingsplicht voor persoonsgegevens indien een dergelijke beperking noodzakelijk is om een van de in artikel 13 van richtlijn 95/46 genoemde doelstellingen te verwezenlijken (zie bijvoorbeeld HvJEU, 29 januari 2008, *Promiscue*, §§ 53-54). Sinds de inwerkingtreding van de AVG moet deze verwijzing naar artikel 13 van richtlijn 95/46 worden gelezen als een verwijzing naar artikel 23 van de AVG (zie artikel 94 van de AVG).

⁶ Zie met name HvJEU, 8 april 2014, *gevoegde zaken C-293/12 en C-594/12 "Digital Rights Ireland et al."*; HvJEU, 21 december 2016, *gevoegde zaken C-203/15 en C-698/15 "Tele2 Sverige et al."*; HvJEU, 2 oktober 2018, *zaak C-207/16, Ministerio Fiscal*; HvJEU, 2 oktober 2020, *gevoegde zaken C-511/18, C-512/18 en C-520/18 "Quadrature du Net et al."*; HvJEU, 2 maart 2021, *zaak C-746/18 "Prokuratuur"*.

⁷ HvJEU, 2 oktober 2020, *gevoegde zaken C-511/18, C-512/18 en C-520/18, "Quadrature du Net et al."*; § 167; HvJEU, 2 maart 2021; HvJEU, 2 maart 2021, *zaak C-746/18, "Prokuratuur"*, § 29.

erop aan dat het wetsontwerp daadwerkelijk de door de jurisprudentie van het HvJEU en het Grondwettelijk Hof vereiste perspectiefwijziging tot stand brengt en derhalve geen nieuwe maatregelen kan opleggen voor het bewaren van verkeers- en lokalisatiegegevens die zouden leiden tot de herinvoering, *de facto*, van verplichtingen inzake de veralgemeende en ongedifferentieerde bewaring van de gegevens. Bij ontstentenis daarvan zou zowel het bewaren van verkeers- en lokalisatiegegevens door de operatoren als de mededeling ervan aan de autoriteiten een inbreuk vormen op de e-Privacyrichtlijn, geïnterpreteerd in het licht van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie.

8. Hoewel de Autoriteit in dit verband geen grondige analyse heeft verricht van de herziene versie van het wetsvoorstel betreffende het verzamelen en bewaren van telecomgegevens, die als bijlage was gevoegd bij de drie adviesaanvragen inzake de bepalingen van het wetsvoorstel die bepaalde autoriteiten toegang willen geven tot de door de operatoren bewaarde verkeers- en lokalisatiegegevens, **wijst een eerste, niet-exhaustieve lezing van deze herziene versie erop dat er nog steeds problemen zijn**⁸. Om ervoor te zorgen dat de overheidsinstanties toegang kunnen hebben tot de door de telecomoperatoren bewaarde gegevens, met naleving van de e-Privacyrichtlijn, **moet er in eerste instantie voor worden gezorgd dat de reglementering inzake de gegevensbewaring voldoet aan de eisen van de e-Privacyrichtlijn**, zoals uitgelegd door het HvJEU.
9. In de tweede plaats herinnert het HvJEU er overeenkomstig het vereiste van voorzienbaarheid aan dat **de mededeling aan de nationale autoriteiten** van door de operatoren bewaarde gegevens **moet worden beheerst door duidelijke en nauwkeurige regels die de omstandigheden en voorwaarden aangeven waaronder deze mededeling plaatsvindt**. Deze reglementering moet voorzien in materiële en procedurele voorwaarden om ervoor te zorgen dat de toegang tot de bewaarde gegevens beperkt blijft tot wat strikt noodzakelijk is⁹:
 - In de **reglementering moet worden bepaald voor welk doel de autoriteiten toegang kunnen krijgen tot de gegevens die worden bewaard** door de aanbieders van communicatiediensten. In dit verband stelt het Hof dat **de toegang tot de gegevens in principe alleen kan worden gerechtvaardigd door het doel van algemeen belang waarvoor de bewaring werd opgelegd**¹⁰. Aldus kan in geen geval toegang worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring ervan is

⁸ De Autoriteit heeft onder meer vastgesteld dat het herziene wetsvoorstel de verplichtingen handhaaft om systematisch verkeersgegevens van alle gebruikers van elektronische-communicatiemiddelen te bewaren, zodat fraude of kwaadwillig gebruik van het netwerk of de dienst kan worden vastgesteld of de dader en oorsprong ervan kunnen worden achterhaald (nieuw artikel 122, § 4 van de Telecomwet) en om de veiligheid en de goede werking van elektronische-communicatienetwerken en -diensten te waarborgen, en met name om een potentiële of feitelijke inbreuk op die veiligheid op te sporen en te analyseren, met inbegrip van het achterhalen van de oorsprong van die inbreuk (nieuw artikel 122, § 4/1 van de Telecomwet).

⁹ HvJEU, arrest van 21 december 2016, §§ 118-121.

¹⁰ HvJEU, arrest van 2 maart 2021, § 31.

gerechtvaardigd door het doel de zware criminaliteit te bestrijden of, *a fortiori*, de nationale veiligheid te waarborgen. Anderzijds kan, overeenkomstig het evenredigheidsbeginsel, de toegang tot gegevens die worden bewaard met het oog op de bestrijding van zware criminaliteit, mits aan de materiële en procedurele voorwaarden voor die toegang is voldaan, worden gerechtvaardigd door de doelstelling van waarborging van de nationale veiligheid. Voorts aanvaardt het Hof dat de Staten kunnen bepalen dat gegevens die worden bewaard op een wijze die in overeenstemming is met de artikelen 5, 6, 9 of 15 van de e-Privacyrichtlijn, met naleving van de materiële en procedurele voorwaarden, aan de autoriteiten mogen worden verstrekt ter bestrijding van de zware criminaliteit of ter vrijwaring van de nationale veiligheid¹¹. De wetgever kan derhalve bepalen dat de autoriteiten op grond van de nieuwe artikelen 122 en 123 van de Telecomwet toegang hebben tot gegevens die worden bewaard voor andere doeleinden dan die waarvoor zij oorspronkelijk zijn bewaard, maar alleen indien die doeleinden van verdere verwerking verband houden met de waarborging van de nationale veiligheid of de bestrijding van de zware criminaliteit, of een ander in artikel 15 van de e-Privacyrichtlijn genoemd doel dat even zwaarwichtig is.

- **De reglementering moet gebaseerd zijn op objectieve criteria om de omstandigheden en voorwaarden vast te stellen waaronder toegang tot de gegevens moet worden toegestaan**¹². In dit verband kan, in verband met de doelstelling van de criminaliteitsbestrijding, in beginsel alleen toegang worden verleend tot gegevens van personen die ervan worden verdacht een strafbaar feit te beramen, te plegen of te hebben gepleegd, of op enigerlei wijze bij een dergelijk strafbaar feit betrokken te zijn. In specifieke situaties, zoals wanneer vitale belangen van de nationale veiligheid, defensie of openbare veiligheid worden bedreigd door terroristische activiteiten, kan echter ook toegang tot de gegevens van andere personen worden verleend wanneer er objectieve elementen zijn om aan te nemen dat deze gegevens in een concreet geval een effectieve bijdrage zouden kunnen leveren aan de bestrijding van dergelijke activiteiten.
- **De toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens moet in principe, behalve in naar behoren gemotiveerde spoedeisende gevallen, worden onderworpen aan een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit**¹³. De beslissing van die rechterlijke instantie of die entiteit moet worden genomen na een met redenen omkleed verzoek van die autoriteiten¹⁴. Voorts heeft het Hof beklemtoond dat de met de voorafgaande toetsing belaste autoriteit, ongeacht of het gaat om een rechterlijke instantie dan wel om een onafhankelijke bestuurlijke entiteit, de

¹¹ HvJEU, arrest van 6 oktober 2020, §§ 164-165.

¹² HvJEU, arrest van 2 maart 2021, § 50.

¹³ In zijn arrest van 2 maart 2021 stelt het HvJEU dat de bestaansreden van deze voorafgaande toetsing (door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit) tot doel heeft de verschillende betrokken belangen *in concreto* met elkaar te verzoenen, met name door ervoor te zorgen dat alleen de gegevens worden meegedeeld die strikt noodzakelijk zijn voor de verwezenlijking van de doelstelling van algemeen belang waarvoor toegang wordt verleend (zie §§ 50-51).

¹⁴ HvJEU, arrest van 21 december 2018, § 120; HvJEU, arrest van 2 maart 2021, § 51.

hoedanigheid van een derde moet hebben ten opzichte van de autoriteit die om toegang tot de gegevens verzoekt, zodat de eerstgenoemde autoriteit deze toetsing onpartijdig en vrij van elke externe beïnvloeding kan verrichten¹⁵. **Het Belgische Grondwettelijk Hof** is echter, voortbouwend op de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: 'EHRM')¹⁶, van oordeel dat **geen voorafgaande toetsing vereist is voor de toegang tot eenvoudige identificatiegegevens**. Voor toegang tot deze gegevens is een toetsing *a posteriori* door een rechterlijke instantie of door een onafhankelijke bestuurlijke instantie voldoende¹⁷.

- **De autoriteiten die toegang tot de gegevens hebben gehad, moeten de betrokkenen daarvan in kennis stellen zodra die bekendmaking het door die autoriteiten verrichte onderzoek niet langer in gevaar kan brengen.** Deze informatie is in feite noodzakelijk om de betrokkenen in staat te stellen met name het recht van verhaal uit te oefenen, waarin uitdrukkelijk is voorzien in artikel 15, § 2 van de e-Privacyrichtlijn, gelezen in samenhang met de AVG, in geval van schending van hun rechten¹⁸. Het **Grondwettelijk Hof** is evenwel van oordeel, voortbouwend op de jurisprudentie van het EHRM, dat het **niet nodig is dat de betrokkene in kennis wordt gesteld van de toegang tot zijn identificatiegegevens**¹⁹.

10. Om de doeltreffendheid van het recht op bescherming van persoonsgegevens en de door de e-Privacyrichtlijn verleende rechten te waarborgen, meent de Autoriteit dat er moet worden bepaald dat **de metagegevens** van elektronische communicatie **die onrechtmatig verkregen zijn, niet mogen worden gebruikt tegen de betrokkene** in het kader van een procedure die impliceert dat ten aanzien van de betrokkene een dwangbesluit wordt genomen.
11. In het vervolg van het advies zal de Autoriteit onderzoeken in hoeverre de bepalingen van het ontwerp aan deze vereisten voldoen.
12. Voorafgaand aan dit onderzoek wenst de Autoriteit echter te benadrukken **dat het van belang is te zorgen voor een zekere mate van transparantie ten aanzien van de praktijk van de overheidsinstanties met betrekking tot de toegang tot en het gebruik van de metagegevens** van elektronische communicatie. Een dergelijke transparantie is immers noodzakelijk om **controle op deze praktijk** door het parlement en het maatschappelijk middenveld mogelijk te maken. Het is wel zo dat het nieuwe artikel 127/1, § 7 van de Telecomwet, dat zal worden ingevoegd door het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens, reeds bepaalt dat het BIPT moet overgaan tot het doorgeven *"annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles*

¹⁵ HvJEU, arrest van 2 maart 2021, § 52.

¹⁶ Zie het arrest van het EHRM, Breyer t. Duitsland, 30 januari 2020.

¹⁷ GwH, arrest nr. 158/2021 van 18 november 2021, § B.14.3.

¹⁸ HvJEU, arrest van 21 december 2018, § 121.

¹⁹ GwH, arrest nr. 158/2021 van 18 november 2021, § B.14.3.

122, 123, 126, 126/1 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants." Volgens deze nieuwe bepaling van de Telecomwet geldt het volgende: "*Ces statistiques comprennent notamment: 1° les cas dans lesquels des données conservées ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ; 2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ; 3° les cas dans lesquels des demandes de données conservées n'ont pu être satisfaites.*" De Autoriteit benadrukt dat **de krachtens artikel 127/1, § 1, van de Telecomwet te verstrekken informatie niet volstaat om het parlement en het maatschappelijk middenveld in staat te stellen controle uit te oefenen op het strikt noodzakelijke en evenredige karakter** van de bepalingen inzake de bewaarplicht en de mededelingsplicht met betrekking tot metagegevens. Artikel 127/1, § 7 (nieuw) van de Telecomwet zou dus moeten worden gewijzigd teneinde op te leggen dat de statistieken die het BIPT jaarlijks moet overmaken aan de minister van Telecommunicatie en de minister van Justitie ook betrekking hebben op (1) het aantal toegangen dat aan de verschillende overheidsinstanties is verleend, (2) het aantal doorgegeven metadata, (3) het aantal personen dat bij die toegangen betrokken was en (4) de mate waarin die toegangen daadwerkelijk nodig zijn gebleken om de instanties in staat te stellen de opdrachten uit te voeren waarvoor zij waren toegestaan. Bovendien moet **aan de verschillende overheidsinstanties die gemachtigd zijn om toegang te hebben tot de metagegevens** van elektronische communicatie **worden opgelegd om jaarlijks statistieken te publiceren** over (1) het aantal toegangen dat hun werd toegestaan, (2) het aantal metagegevens waartoe zij toegang hebben gehad, (3) het aantal personen dat bij die toegang betrokken was, (4) de impact van die toegangen op de uitoefening van hun opdrachten (bv. in welke mate de toegang tot de metagegevens het daadwerkelijk mogelijk heeft gemaakt het onderzoek tot een goed einde te brengen). **Het wetsontwerp moet worden aangepast om een dergelijke verplichting tot publicatie van statistieken voor de BMA, de FOD Economie en het NIS op te nemen.**

B. Toegang tot gegevens door de Belgische mededingingsautoriteit (CO-A-2021-280)

13. Bij **artikel 7 van het wetsontwerp** wordt een nieuwe **paragraaf 1/1 ingevoegd in artikel IV.40** van het Wetboek van Economisch Recht (hierna 'het WER'). Deze nieuwe bepaling moet **de auditor van de BMA** in staat stellen om bij de telecomoperatoren **verkeersgegevens, lokalisatiegegevens, identificatiegegevens of -documenten en IP-adressen** op te vragen die worden beoogd in het nieuwe artikel 127/1, §§ 2 en 3 van de Telecomwet²⁰, indien dit noodzakelijk is

²⁰ De in het nieuwe artikel 127/1, §§ 2 en 3 bedoelde gegevens zijn de gegevens die de operatoren bewaren ter uitvoering van de nieuwe artikelen 122, 123, 126 en 127. Het gaat met name om de verkeersgegevens die nodig zijn voor de facturering van abonnees of het doen van interconnectiebetalingen, verkeersgegevens, met inbegrip van lokalisatiegegevens (artikel 122, § 2), verkeersgegevens die noodzakelijk zijn om de marketing te verzorgen van de eigen elektronische-communicatiediensten en om het gebruikspatroon op te stellen van de abonnee of de eindgebruiker (artikel 122, § 3), lokalisatiegegevens en andere

voor de vervolging van inbreuken op de artikelen 101 en 102 VWEU en de artikelen IV.1, IV.2 en IV.2/1 en voor het concentratietoezicht. In de ontwerpbepaling wordt gespecificeerd dat de vervolging van dergelijke inbreuken en het concentratietoezicht *"strekken tot het vrijwaren van een belangrijk economisch belang van de Europese Unie of van België"*.

14. De Autoriteit stelt vast dat de **ontwerpbepaling**, die tot doel heeft de voorwaarden te regelen waaronder de BMA toegang kan krijgen tot de gegevens, **voldoet aan de door het HvJEU vastgestelde basisvereisten**.
15. Ten eerste **bepaalt de ontwerpbepaling voor welke doeleinden** de BMA toegang kan krijgen tot de bewaarde gegevens, namelijk de vervolging van inbreuken op de artikelen 101 en 102 VWEU en op de artikelen IV.1, IV.2 en IV.2/1 en het concentratietoezicht; dit strekt tot *"het vrijwaren van een belangrijk economisch belang van de Europese Unie of van België"*.
16. De Autoriteit stelt ook vast dat **de reglementering**, in overeenstemming met de jurisprudentie van het HvJEU, **voorziet in objectieve criteria om de omstandigheden en voorwaarden te bepalen waaronder toegang tot de gegevens moet worden verleend**. Krachtens artikel IV.40, § 1 WER kan de auditor *"alle noodzakelijke inlichtingen"* inwinnen met het oog op het uitvoeren van zijn opdrachten, *in casu* de vervolging van inbreuken op de artikelen 101 en 102 VWEU en de artikelen IV.1, IV.2 en IV.2/1 en het concentratietoezicht. Bovendien bepaalt dit artikel dat in het verzoek om inlichtingen de rechtsgrondslag en het *"doel"* van het verzoek moeten worden vermeld. Volgens de door de afgevaardigde van de minister verstrekte informatie **moet het begrip "noodzakelijke inlichtingen" worden uitgelegd als inlichtingen aan de hand waarvan de auditor de vermoedens van een inbreuk die de uitvoering van het onderzoek rechtvaardigen, kan verifiëren**. Er wordt met andere woorden bepaald dat de BMA slechts toegang kan verkrijgen tot de verkeersgegevens, lokalisatiegegevens, identificatiegegevens en IP-adressen in de mate dat deze gegevens haar in staat stellen vermoedens van een inbreuk te verifiëren. **De Autoriteit neemt hier nota van**.
17. Bovendien wordt in de ontwerpbepaling het volgende vastgelegd: *"De verstrekking van deze gegevens kan slechts worden gevorderd op gemotiveerd verzoek en met voorafgaande machtiging van een onderzoeksrechter in de Nederlandstalige rechtbank van eerste aanleg te Brussel of een onderzoeksrechter in de Franstalige rechtbank van eerste aanleg te Brussel, die voor de toepassing*

verkeersgegevens die nodig zijn voor de opsporing en de analyse van vermoedelijke fraude of vermoedelijk kwaadwillig gebruik van het netwerk (artikel 122, § 4), verkeersgegevens die nodig zijn om de veiligheid en de correcte werking van het netwerk en de diensten voor elektronische communicatie te garanderen (artikel 122, § 4/1), andere lokalisatiegegevens dan de verkeersgegevens (artikel 123), abonnementsgegevens van de abonnee voor de dienst en de gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren (artikel 126) en de identificatiegegevens en -documenten van de eindgebruiker (artikel 127).

van dit lid ook bevoegd is buiten zijn arrondissement." **Elke toegang tot de gegevens is dus onderworpen aan de voorafgaande toetsing door de onderzoeksrechter**, die, volgens de aanvullende toelichtingen van de afgevaardigde van de minister, zal onderzoeken of het verzoek van de BMA om toegang gerechtvaardigd is, met name door zich ervan te vergewissen dat de BMA daadwerkelijk over voldoende overeenstemmende en ernstige aanwijzingen beschikt om een inbreuk op de artikelen 101 en 102 VWEU en de artikelen IV.1, IV.2 en IV.2/1 en het concentratietoezicht te vermoeden. **De Autoriteit neemt hier nota van.**

18. Tot slot heeft de gemachtigde van de minister aan de Autoriteit, naar aanleiding van een verzoek om aanvullende inlichtingen, erop gewezen dat boek IV van het WER **waarborgt dat de personen die betrokken zijn bij de mededeling van verkeersgegevens, lokalisatiegegevens, identificatiegegevens of -documenten en IP-adressen, van deze mededeling in kennis worden gesteld** zodra deze informatie het door deze autoriteiten verrichte onderzoek niet langer in gevaar kan brengen, dat wil zeggen op het moment dat de partijen inzage kunnen krijgen in het onderzoekdossier. **De Autoriteit neemt hier nota van.**
19. De Autoriteit herinnert eraan dat om de doeltreffendheid van het recht op bescherming van persoonsgegevens en de rechten die de betrokkenen ontleen aan de e-Privacyrichtlijn te waarborgen, er moet worden bepaald, in het WER, dat **de metagegevens** van elektronische communicatie **die onrechtmatig verkregen zijn** door de BMA, **niet mogen worden gebruikt tegen de betrokkene** in het kader van een procedure die impliceert dat ten aanzien van de betrokkene een dwangbesluit wordt genomen.

C. Toegang tot gegevens door de ambtenaren van de economische inspectie (CO-A-2021-281)

20. Artikel 25, 1° van het wetsontwerp beoogt artikel XV.3, 5/1° van het WER aan te vullen om **de ambtenaren van de EI onder bepaalde voorwaarden toe te staan toegang te krijgen:**
 - (1) tot **identificatiedocumenten en -gegevens** die door de telecomoperatoren worden bewaard **om te kunnen overgaan tot de identificatie** van natuurlijke of rechtspersonen **aan de hand van het telefoonnummer van de betrokkene of het IP-adres**,
 - (2) tot de **verkeersgegevens, lokalisatiegegevens en IP-adressen**, zoals bedoeld in en in overeenstemming met artikel 127/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie **in het kader van het onderzoek en de vaststelling van strafbare feiten van niveau 5 of 6.**

- i) *Met betrekking tot de mogelijkheid voor de ambtenaren van de EI om toegang te krijgen tot de documenten en identificatiegegevens die door de telecomoperatoren worden bewaard, met het oog op de identificatie van natuurlijke of rechtspersonen aan de hand van het telefoonnummer van de betrokkene of het IP-adres*

21. De **ontwerpbepaling** strekt ertoe de ambtenaren van de EI die belast zijn met het onderzoek en de vaststelling van inbreuken op het WER **toegang te verlenen tot de identificatiedocumenten en -gegevens** waarover de telecomoperatoren beschikken om natuurlijke of rechtspersonen aan de hand van **een telefoonnummer** of een **IP-adres te kunnen identificeren**. Hier gaat het dus om het opleggen van de verplichting aan de operatoren om aan de ambtenaren van de EI de identificatiegegevens mee te delen:
- van de houder van het telefoonnummer met behulp waarvan een inbreuk op het WER zou zijn gepleegd,
 - van de houder van een dienstenovereenkomst voor internettoegang aan wie het IP-adres is toegewezen dat is geïdentificeerd als het adres dat is toegewezen aan het op internet aangesloten apparaat met behulp waarvan een inbreuk op het WER zou zijn gepleegd.
22. Ten eerste merkt de Autoriteit op dat volgens de rechtspraak van het HvJEU **de toegang van een overheidsinstantie tot de identificatiedocumenten en -gegevens** die bewaard worden door een telecomoperator met als **enig doel** de betrokken gebruiker te **identificeren, een inmenging** vormt in het recht op privacy **die niet als 'ernstig' kan worden aangemerkt**. Bijgevolg geeft het HvJEU toe dat **een dergelijke inmenging kan worden gerechtvaardigd door een doelstelling van preventie, onderzoek, opsporing en vervolging van inbreuken in het algemeen**, zonder dat deze inbreuken als 'ernstig' moeten worden aangemerkt²¹. Zo heeft het HvJEU geoordeeld dat de toegang van overheidsinstanties tot gegevens ter identificatie van de houders van simkaarten die met een gestolen mobiele telefoon zijn geactiveerd, zoals naam, voornaam en, in voorkomend geval, adres van deze houders, kan worden verleend met het oog op het onderzoeken, opsporen en vervolgen van strafbare feiten, zonder dat deze als 'ernstig' moeten worden aangemerkt²², mits de toegang tot deze gegevens onderworpen is aan de strikte naleving van de materiële en procedurele voorwaarden die voor het gebruik van deze gegevens gelden. De Autoriteit zal hierop terugkomen.
23. Uit de Europese rechtspraak blijkt zeer duidelijk dat een wetgevingsmaatregel, die ertoe strekt ambtenaren van de EI in staat te stellen identificatiedocumenten en -gegevens te verkrijgen die door een telecomoperator worden bewaard om de betrokken gebruiker te kunnen identificeren **op basis van een telefoonnummer** dat zij aan de operator bezorgen, een passende, noodzakelijke en evenredige maatregel is, **op voorwaarde evenwel dat bij deze toegang de andere materiële**

²¹ Zie met name HvJEU, 6 november 2020, §§ 157 en 158.

²² HvJEU, 2 oktober 2018, §§ 48-63.

en procedurele voorwaarden die voor het gebruik van dergelijke gegevens moeten gelden, in acht worden genomen (*cf. infra*).

24. Op het eerste gezicht lijkt de kwestie **delicater** wat betreft **de mogelijkheid om door een operator bewaarde identificatiedocumenten en -gegevens te verkrijgen op basis van een IP-adres** dat door de ambtenaren van de EI wordt meegedeeld. Om de operatoren in staat te stellen de persoon aan wie dit adres op een bepaald tijdstip werd toegekend, te identificeren en vervolgens de identificatiedocumenten en -gegevens aan de ambtenaren van de EI door te geven, is het immers noodzakelijk dat de IP-adressen ook na de toekenningsperiode worden bewaard. In zijn arrest van 6 oktober 2020 heeft het HvJEU echter geoordeeld dat een wetgevingsmaatregel alleen een verplichting mag opleggen om de aan de bron van een verbinding toegewezen IP-adressen algemeen en ongedifferentieerd te bewaren in het kader van de bestrijding van zware criminaliteit (of met het oog op het bereiken van een van de doelstellingen van artikel 15 van de e-Privacyrichtlijn die van vergelijkbaar belang zijn), gelet op de ernst van de inmenging in het recht op eerbiediging van de persoonlijke levenssfeer die wordt veroorzaakt door het algemeen en ongedifferentieerd bewaren van de IP-adressen die aan de bron van een verbinding zijn toegewezen²³. Zoals het HvJEU echter zelf erkent, kan in het geval van een online gepleegd strafbaar feit het IP-adres dat is toegewezen aan de bron van een verbinding, het enige onderzoeksmiddel zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd²⁴. In deze omstandigheden is de **Autoriteit van mening dat de mededeling van documenten en identificatiegegevens** van de abonnee die door de operator is geïdentificeerd **vanaf een IP-adres** dat op een bepaald moment aan hem is toegekend, een **noodzakelijke, passende en evenredige maatregel** kan vormen, **op voorwaarde** evenwel dat deze **mededeling** wordt onderworpen aan de strikte naleving van **de materiële en procedurele voorwaarden** die het gebruik van die gegevens moeten beheersen (*cf. infra*).
25. In dit verband merkt de Autoriteit in de eerste plaats op dat **de reglementering**, in overeenstemming met de jurisprudentie van het HvJEU, **de omstandigheden en de voorwaarden definieert waaronder toegang tot de identificatiegegevens kan worden verleend**²⁵. Artikel XV.3, 5^o/1, eerste lid WER bepaalt immers dat de ambtenaren van de EI *"zich op eerste vordering door elke persoon gratis alle inlichtingen [kunnen] laten verstrekken die de identificatie mogelijk maken van personen die het voorwerp uitmaken van een onderzoek en personen die betrokken zijn bij financiële en gegevensstromen die noodzakelijk zijn in het kader van het onderzoek"*. In de ontwerpbeoordeling wordt naar aanleiding van dit lid het volgende ingevoegd: *"Voor wat de identificatie betreft van*

²³ De ernst van de inmenging wordt gerechtvaardigd door het volgende feit: *"Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld"* (§ 153).

²⁴ HvJEU, 6 oktober 2020, § 154.

²⁵ HvJEU, arrest van 2 maart 2021, § 50.

natuurlijke of rechtspersonen aan de hand van het telefoonnummer van de betrokkene of het IP-adres, kunnen zij, [...], de verstrekking van de identificatiedocumenten en -gegevens vorderen van de operator [...]."

26. Vervolgens stelt de Autoriteit vast dat de ontwerpbeplanning voorziet in een interne voorafgaande toetsing binnen de overheidsdienst, aangezien elk verzoek om toegang tot de identificatiegegevens en -documenten (1) moet worden gevalideerd door de leidend ambtenaar of zijn vertegenwoordiger en (2) moet worden toegestaan door andere ambtenaren van de EI dan die welke het verzoek hebben ingediend, aan wie wordt gevraagd de noodzaak en de evenredigheid van de maatregel te controleren. Er is in deze zaak dus niet voorzien in een voorafgaande toetsing door een dergelijke rechterlijke instantie of onafhankelijke bestuurlijke autoriteit. Hoewel het bij het lezen van de rechtspraak van het HvJEU niet duidelijk is dat het ontbreken van een dergelijke voorafgaande toetsing naar Europees recht geoorloofd is, merkt de Autoriteit op dat het Grondwettelijk Hof, voortbouwend op de rechtspraak van het EHRM, van oordeel is dat het niet vereist is om een toezicht *a priori* te organiseren om toegang te krijgen tot eenvoudige identificatiegegevens. Onder deze voorwaarden **neemt de Autoriteit nota van de beslissing** van de auteur van het ontwerp om **niet te voorzien in een toetsing die voorafgaat aan de mededeling van de identificatiedocumenten en -gegevens** van de abonnee die door de operator is geïdentificeerd op basis van een IP-adres of een telefoonnummer.
27. De Autoriteit benadrukt evenwel dat het essentieel is dat de maatregelen van interne controle ervoor zorgen dat de ambtenaren van de EI alleen toegang hebben tot de identificatiegegevens en -documenten van personen die aan de hand van een telefoonnummer of IP-adres zijn geïdentificeerd, indien zij, gelet op de feiten, beschikken over een reeks overeenstemmende en ernstige aanwijzingen dat deze identificatiegegevens het onderzoek naar en de vaststelling van inbreuken op het WER mogelijk zouden maken of zouden bespoedigen. Bovendien benadrukt de Autoriteit dat **de identificatie van een persoon aan de hand van een telefoonnummer of IP-adres het mogelijk maakt de persoon te identificeren die is geabonneerd op de betrokken elektronische-communicatiedienst, maar die niet noodzakelijkerwijs overeenstemt met de persoon die het strafbare feit pleegt of daarbij betrokken is**. Het is van essentieel belang dat de ambtenaren van de EI zich ervan bewust zijn dat het voor de geïdentificeerde persoon die niet bij het strafbare feit betrokken is, misschien niet mogelijk is (negatief) bewijs te leveren daarvoor. De Autoriteit geeft bijgevolg aan dat, afhankelijk van de omstandigheden van de zaak, aanvullende onderzoekshandelingen ter identificatie van de houder van het rekeningnummer of het contract voor internettoegang nodig kunnen zijn om vermoedelijke strafbare feiten die zijn gepleegd met gebruikmaking van een elektronisch communicatiemiddel te bevestigen.

ii) *Wat betreft de mogelijkheid voor de ambtenaren van de EI om toegang te hebben tot verkeersgegevens, lokalisatiegegevens en IP-adressen in het kader van het onderzoek naar en de vaststelling van strafbare feiten van niveau 5 of 6*

28. Het nieuwe artikel XV.3, 5/1°, laatste lid, van het WER, ingevoegd bij artikel 25, 1° van het wetsontwerp, beoogt de ambtenaren van het EI, belast met het onderzoek en de vaststelling van inbreuken op het WER, onder bepaalde voorwaarden toegang te verlenen tot verkeersgegevens, lokalisatiegegevens en IP-adressen die door de operatoren worden bewaard ter uitvoering van de (nieuwe) artikelen 122, 123, 126, 126/1 en 127 van de Telecomwet. In de ontwerp-bepaling wordt gespecificeerd dat *"de verkeers- en lokalisatiegegevens [...] slechts opgevraagd [kunnen] worden voor het opsporen en vaststellen van inbreuken van niveau 5 of 6"*, met andere woorden de inbreuken die worden bestraft met de zwaarste straffen.
29. De Autoriteit stelt vast dat de **ontwerpbepaling**, die tot doel heeft de voorwaarden te regelen waaronder ambtenaren van de EI toegang kunnen krijgen tot verkeersgegevens, lokalisatiegegevens en IP-adressen, zoals bedoeld in artikel 127/1 van de Telecomwet, **in wezen voldoet aan de door het HvJEU vastgestelde basisvereisten**.
30. In de eerste plaats bepaalt de **ontwerpbepaling** – gelezen in samenhang met artikel XV.2 van het WER – de doeleinden waarvoor de ambtenaren van het EI toegang kunnen krijgen tot de bewaarde gegevens, namelijk het onderzoek naar en de vaststelling van inbreuken op het WER van niveau 5 of 6 (met uitzondering van de in boek IV en de uitvoeringsbesluiten daarvan genoemde inbreuken). De mogelijkheid om alleen toegang te krijgen tot verkeers- en lokalisatiegegevens voor het onderzoeken en vaststellen van strafbare feiten van niveau 5 of 6, d.w.z. die welke als de ernstigste worden beschouwd, is in overeenstemming met de jurisprudentie van het HvJEU. **In de ontwerpbepaling moeten echter alle dubbelzinnigheden worden weggewerkt met betrekking tot het feit dat de IP-adressen ook enkel aan de ambtenaren van de EI mogen worden verstrekt met het oog op het onderzoeken en vaststellen van inbreuken op het WER van niveau 5 of 6.**
31. De Autoriteit stelt vast dat de ontwerpbepaling *"les adresses IP, telles que visées par l'article 127/1 de la loi du 13 juin 2005 relatives aux communications électroniques"* beoogt. Deze bepaling van de Telecomwet verwijst naar de gegevens die worden bewaard ter uitvoering van de artikelen 126 (nieuw) en 127 (nieuw). Het nieuwe artikel 126 heeft betrekking op de bewaring van abonnementsgegevens en gegevens die nodig zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische communicatiedienst te identificeren. Het delegeert aan de Koning de bevoegdheid om een lijst op te stellen van de precieze gegevens die door de operatoren moeten worden bewaard, maar specificeert dat deze gegevens geen betrekking mogen hebben *"sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le*

*destinataire de la communication, comme l'adresse IP du destinataire de la communication ou sur la localisation de l'équipement terminal*²⁶. Krachtens het nieuwe artikel 126 van de Telecomwet kan de Koning alleen de bewaring opleggen van de IP-adressen die zijn toegewezen aan de bron van de verbinding. **De ambtenaren van de EI kunnen dus, ter uitvoering van het nieuwe artikel XV.3, 5/1°, laatste lid, van het WER, enkel toegang hebben tot de IP-adressen die zijn toegewezen aan de bron van de verbinding, met uitzondering van de IP-adressen van de geadresseerde van de communicatie.** Bovendien moet worden opgemerkt dat in het nieuwe artikel 127/1, § 3, vierde lid, van de Telecomwet het volgende wordt gespecificeerd: *"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"*²⁷. Deze beperking inzake het soort IP-adressen dat aan de autoriteiten kan worden verstrekt (met name alleen de IP-adressen die zijn toegewezen aan de bron van de verbinding en alleen voor zover de autoriteit die om toegang verzoekt, niet anderszins over informatie beschikt waarmee zij de navigatieroute van een eindgebruiker op het internet kan traceren) is absoluut essentieel om de evenredigheid te waarborgen van de inmenging in het recht op privacy die wordt veroorzaakt door de bewaring van en de toegang tot metagegevens.

32. In overeenstemming met de jurisprudentie van het HvJEU **stelt de reglementering de omstandigheden en voorwaarden vast waaronder toegang tot de identificatiegegevens moet worden verleend**²⁸. Artikel XV.3, 5°/1, eerste lid WER bepaalt immers dat de ambtenaren van de IE *"zich op eerste vordering door elke persoon gratis alle inlichtingen [kunnen] laten verstrekken die de identificatie mogelijk maken van personen die het voorwerp uitmaken van een onderzoek en personen die betrokken zijn bij financiële en gegevensstromen die noodzakelijk zijn in het kader van het onderzoek"*. De ambtenaren van de EI kunnen dus toegang krijgen tot de gegevens onder de strikte voorwaarde dat ze noodzakelijk zijn in het kader van het onderzoek.
33. Bovendien bepaalt de bepaling van het ontwerp het volgende: *"Verkeersgegevens, locatiegegevens en IP-adressen, zoals bedoeld in en in overeenstemming met artikel 127/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, kunnen slechts opgevraagd worden op gemotiveerd verzoek en met voorafgaande machtiging van een onderzoeksrechter in de Nederlandstalige rechtbank van eerste aanleg te Brussel of een onderzoeksrechter in de Franstalige rechtbank van eerste aanleg te Brussel [...]"*. Elke toegang tot de gegevens is bijgevolg, overeenkomstig de jurisprudentie van het

²⁶ Onderlijning door de Autoriteit

²⁷ Onderlijning door de Autoriteit

²⁸ HvJEU, arrest van 2 maart 2021, § 50.

HvJEU, onderworpen aan de voorafgaande toetsing door de onderzoeksrechter. **De Autoriteit neemt hier nota van.** Hij herinnert eraan dat de onderzoeksrechter alleen verplicht is toegang tot verkeers- en lokalisatiegegevens te verlenen indien er, gelet op de feiten, een geheel van overeenstemmende en ernstige aanwijzingen bestaat dat de opgevraagde persoonsgegevens het onderzoek naar en de vaststelling van strafbare feiten in de zin van het COB mogelijk zouden maken of zouden bespoedigen.

34. **De auteur van het wetsontwerp moet er tot slot voor zorgen dat het regelgevingskader waarborgt dat de personen op wie de mededeling van hun identificatiegegevens betrekking heeft, van deze mededeling in kennis worden gesteld** zodra deze informatie het door deze autoriteiten verrichte onderzoek niet langer in gevaar kan brengen. Indien het materieel recht hier nog niet in voorziet, moet het regelgevingskader worden aangepast om ervoor te zorgen dat de betrokkenen over de vereiste informatie beschikken.
35. De Autoriteit herinnert eraan dat om de doeltreffendheid van het recht op bescherming van persoonsgegevens en de rechten die de betrokkenen ontleen aan de e-Privacyrichtlijn te waarborgen, er moet worden bepaald dat **de metagegevens** van elektronische communicatie **die onrechtmatig verkregen zijn** door de ambtenaren van de EI, **niet mogen worden gebruikt tegen de betrokkene** in het kader van een procedure die impliceert dat ten aanzien van de betrokkene een dwangbesluit wordt genomen.

D. Toegang tot de gegevens door het Nationaal Instituut voor de Statistiek (CO-A-2021-283)

36. Artikel 47 van het wetsontwerp strekt tot invoeging van een nieuw artikel 24^{sexies} in de wet van 4 juli 1962 betreffende de openbare statistiek (hierna 'de wet van 4 juli 1962'). Met deze **nieuwe bepaling** wordt beoogd **het NIS te machtigen**, *"overeenkomstig artikel 127/1, § 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, voor statistische doeleinden door de operatoren bewaarde gegevens te verwerken en te onderzoeken"*.
37. Het nieuwe artikel 127/1, § 2, 10°, van de Telecomwet, dat in werking zal treden na de aanneming van het wetsontwerp betreffende de inzameling en de bewaring van telecomgegevens, heeft tot doel *"les autorités qui sont légalement habilités à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques"* toe te staan *"des données conservées en vertu des articles 122 et 123 [...] pour autant que prévu et par et aux conditions fixées par une norme législative formelle"* te verkrijgen.

38. De **gegevens die op grond van de (nieuwe) artikelen 122 en 123 van de Telecomwet worden bewaard, zijn talrijk**. Het gaat met name om de verkeersgegevens die nodig zijn voor de facturering van abonnees of het doen van interconnectiebetalingen, verkeersgegevens, met inbegrip van locatiegegevens (artikel 122, § 2), verkeersgegevens die noodzakelijk zijn om de marketing te verzorgen van de eigen elektronische-communicatiediensten en om het gebruikspatroon op te stellen van de abonnee of de eindgebruiker (artikel 122, § 3), lokalisatiegegevens en andere verkeersgegevens die nodig zijn voor de opsporing en de analyse van vermoedelijke fraude of vermoedelijk kwaadwillig gebruik van het netwerk (artikel 122, § 4), verkeersgegevens die nodig zijn om de veiligheid en de correcte werking van het netwerk en de diensten voor elektronische communicatie te garanderen, (artikel 122, § 4/1), andere lokalisatiegegevens dan de verkeersgegevens (artikel 123).
39. Zoals in de memorie van toelichting terecht wordt opgemerkt, vereist artikel 5.1.b) van de AVG dat persoonsgegevens *"voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden [moeten] worden verzameld en [...] vervolgens niet verder op een met die doeleinden onverenigbare wijze [mogen] worden verwerkt"*, waarbij evenwel wordt erkend dat *"de verdere verwerking met het oog op [...] statistische doeleinden [...] overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden [wordt] beschouwd"*. Volgens artikel 89.1 van de AVG moet de verwerking voor statistische doeleinden onderworpen zijn aan passende waarborgen voor de rechten en vrijheden van de betrokkenen.
40. De **verwerking door het NIS voor statistische doeleinden van de gegevens** die door de operatoren **worden bewaard** overeenkomstig artikel 127/1, § 2, 10° van de Telecomwet, moet bijgevolg, in principe, **verenigbaar worden geacht met de doeleinden waarvoor deze gegevens oorspronkelijk werden bewaard**²⁹.
41. De Autoriteit merkt bovendien op dat de wet van 4 juli 1962, in overeenstemming met artikel 89.1 van de AVG, meerdere passende waarborgen biedt voor de rechten en vrijheden van de betrokkenen³⁰.

²⁹ We herinneren eraan dat het HvJEU in verschillende arresten heeft geoordeeld dat de reglementering moet bepalen voor welk doel de autoriteiten toegang kunnen krijgen tot door de aanbieders van communicatiediensten bewaarde gegevens, met dien verstande dat die toegang in principe alleen kan worden gerechtvaardigd door het doel van algemeen belang waarvoor de bewaring is opgelegd. Hoewel het HvJEU zich nog niet heeft uitgesproken over een reglementering die toegang verleent tot de door de operatoren voor statistische doeleinden bewaarde gegevens, merkt de Autoriteit op dat het in principe niet in strijd lijkt te zijn met de AVG of de e-Privacyrichtlijn om voor statistische doeleinden toestemming te geven voor de mededeling van de door de aanbieders van communicatiediensten bewaarde verkeersgegevens, zelfs indien de bewaring van de gegevens aanvankelijk niet voor statistische doeleinden was opgelegd. De AVG voert in feite een 'voorkeursregime' in voor verdere verwerking voor statistische doeleinden.

³⁰ Deze wet van 4 juli 1962 voorziet in waarborgen voor de betrokkenen, zoals de verplichting de beginselen van rechtmatigheid en behoorlijkheid, finaliteit, evenredigheid en onpartijdigheid, objectiviteit en professionele onafhankelijkheid in acht te nemen, en de verplichting de statistische geheimhouding te waarborgen. Voorts herinnert de Autoriteit eraan dat zij in haar advies nr. 127/2021 van 28 juli 2021 een voorontwerp van wet tot wijziging van de wet van 4 juli 1962 heeft onderzocht. In dat advies heeft de Autoriteit een aantal opmerkingen gemaakt en aanbevelingen gedaan voor wijzigingen om ervoor te zorgen dat de wet op de openbare statistieken de betrokkenen passende adequate waarborgen biedt.

42. De Autoriteit herinnert eraan dat **de verwerking van verkeers- en lokalisatiegegevens** niet alleen moet voldoen **aan** de vereisten van **de GDPR**, maar ook **aan** die van de **e-privacyrichtlijn**, die, zoals bekend, de GDPR specificeert en aanvult wat betreft de verwerking van persoonsgegevens in de elektronische-communicatiesector³¹.
43. Deze **richtlijn** legt onder meer **de waarborging van het vertrouwelijke karakter** op van de verkeersgegevens betreffende de communicaties via een toegankelijk openbaar communicatienetwerk en elektronische-communicatiediensten en van andere lokalisatiegegevens dan de verkeersgegevens.
44. **Het nieuwe artikel 24sexies** van de wet van 4 juli 1962, ingevoerd door artikel 47 van het wetsontwerp, beoogt een **afwijking van het beginsel van vertrouwelijkheid** van verkeers- en lokalisatiegegevens. Dergelijke afwijkingen zijn **alleen** toegestaan **binnen de grenzen van artikel 15.1 van de e-Privacyrichtlijn**. Ter herinnering, artikel 15.1 van de e-Privacyrichtlijn bepaalt het volgende: *"De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, [...] en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG [...]."* Volgens vaste rechtspraak van het HJEU moet de verwijzing naar artikel 13 van Richtlijn 95/46/EG aldus worden gelezen dat de lidstaten maatregelen mogen nemen ter beperking van de verplichting tot vertrouwelijkheid van elektronische communicatie en daarmee verband houdende verkeers- en lokalisatiegegevens, indien een dergelijke beperking noodzakelijk is om een van de in artikel 13 van Richtlijn 95/46/EG genoemde doelstellingen te verwezenlijken³². Sinds de inwerkingtreding van de AVG moet deze verwijzing naar artikel 13 van richtlijn 95/46 worden gelezen als een verwijzing naar artikel 23 van de AVG ³³.
45. Uit de memorie van toelichting bij het wetsvoorstel en de aanvullende inlichtingen die zijn verstrekt door de afgevaardigde van de minister, blijkt dat artikel 47 van het wetsvoorstel **tot doel heeft** het NIS toegang te verlenen tot de door de telecomoperatoren bewaarde gegevens om **statistieken op te stellen over het gebruik van informatie- en communicatietechnologieën door de huishoudens en de ondernemingen**, zoals wordt voorgeschreven door de volgende twee Europese verordeningen: verordening 2019/1700 van het Europees Parlement en de Raad van 10 oktober 2019 tot vaststelling van een gemeenschappelijk kader voor Europese statistieken betreffende personen en huishoudens, op basis van gegevens die op individueel niveau worden verzameld door middel van

³¹ Artikel 1.2 van de e-Privacyrichtlijn. De Autoriteit merkt ook op dat de e-Privacyrichtlijn, in tegenstelling tot de AVG, ook de rechtmatige belangen van de abonnees die rechtspersonen zijn, beoogt te beschermen (artikel 1 van de e-Privacyrichtlijn).

³² Zie bijvoorbeeld HvJEU, 29 januari 2008, Promiscuae, §§ 53-54.

³³ Zie artikel 94 van de AVG.

steekproeven (hierna 'de verordening 2019/1700') en verordening 2019/2152 van het Europees Parlement en de Raad van 27 november 2019 betreffende Europese bedrijfsstatistieken (hierna 'de verordening 2019/2152').

46. De afgevaardigde van de minister deelde naar aanleiding van een verzoek om aanvullende inlichtingen mee **dat voor de opstelling van kwaliteitsvolle statistieken** over het gebruik van informatie- en communicatietechnologieën door huishoudens en ondernemingen **informatie moet worden verzameld, zowel bij de betrokkenen** (via enquêtes) **als bij de telecomoperatoren**. Enerzijds kunnen sommige inlichtingen alleen door middel van enquêtes door de betrokkenen worden verstrekt (bv. gegevens over internetgebruik, gebruik van *e-commerce* of *e-government*-diensten). De uitvoeringsverordeningen van verordening 2019/1700 leggen trouwens op, naar het voorbeeld van uitvoeringsverordening 2021/1223 van de Commissie van 27 juli 2021, dat de relevante gegevens door middel van een enquête worden verzameld. Anderzijds kan de nauwkeurigheid van de via enquêtes verzamelde gegevens problematisch zijn, met name ten aanzien van de volgende elementen:

"De antwoorden van de gezinnen/ondernemingen zijn fout of de gezinnen zijn het antwoord schuldig omdat de informatie te technisch is: De gezinnen/ondernemingen hebben het door de WIFI-technologie moeilijk om een onderscheid te maken tussen vast internet en mobiel internet. Ze denken ten onrechte dat WIFI (draadloos) gelijk staat met mobiel internet waardoor we het aandeel gezinnen met vast internet onderschatten. Door de informatie van de telecomoperatoren te koppelen aan de gegevens van de enquête kunnen we dit corrigeren op het niveau van een case (microniveau). Verder is het voor de gezinnen ook moeilijk om correcte informatie te geven over bijvoorbeeld de snelheid van de internetverbinding of de technologie die ermee samenhangt (bv. klassieke internetconnectie of ADSL).

De resultaten geven geen correct beeld van de volledige bevolking: Bij de enquête werkt ongeveer de helft van de gezinnen die via een steekproef getrokken worden mee. Het al dan niet deelnemen aan een enquête hangt samen met de leeftijd, het geslacht en de socio-economische status. Mensen die tot een lagere sociale klasse behoren, doen minder mee aan enquêtes en de kans is groot dat deze profielen ook minder dan de andere toegang hebben tot internet. Ook taalbarrières, technische barrières (deelnemers begrijpen niet altijd wat wordt bedoeld met "vast", "breedband", enz.) kunnen een vertekening van de resultaten veroorzaken. Om daarvoor te kunnen corrigeren, dienen we voor de totale bevolking (minstens op gezinsniveau) informatie te hebben over de toegang tot

internet en het profiel. Dit laat toe om de resultaten te herwegen (kalibreren) en zo op macroniveau te corrigeren."

47. De Autoriteit **neemt er nota van** dat de door de operatoren bewaarde gegevens kunnen bijdragen tot het waarborgen van de kwaliteit van de gegevens waarop de statistieken over het gebruik van informatie- en communicatietechnologieën worden gebaseerd.
48. De Autoriteit is van oordeel dat de opstelling van dergelijke statistieken overeenkomstig de Verordeningen 2019/1700 en 2019/1952 kan worden aangemerkt als een *"belangrijke doelstelling van algemeen openbaar belang van de Unie of van een lidstaat"*³⁴, die een van de doelstellingen is op grond waarvan het krachtens artikel 15, lid 1, van de e-privacyrichtlijn, gelezen in het licht van artikel 23, lid 1, onder e), van de RAPV, is toegestaan de geheimhoudingsplicht met betrekking tot verkeers- en lokalisatiegegevens in verband met elektronische communicatie te beperken, mits die beperking bovendien noodzakelijk, redelijk en evenredig blijkt te zijn.
49. Met het oog op **voldoende voorzienbaarheid** van de reglementering moet het **concrete statistische doel** waarvoor het NIS toegang kan vragen tot de door de telecomoperatoren bewaarde gegevens zoals bedoeld in het nieuwe artikel 127/1, § 2 van de Telecomwet, **worden opgenomen** in het nieuwe artikel 24^{sexies}, dat bij artikel 47 van het ontwerp wordt ingevoerd. Het **ontwerp moet** dienovereenkomstig **worden aangepast**.
50. Voorts stelt de Autoriteit in dit verband vast dat **de ontwerpbepaling het NIS momenteel toegang verleent tot alle gegevens** die ter uitvoering van de artikelen 122 en 123 van de Telecomwet worden bewaard, en **niet alleen tot de gegevens die noodzakelijk zijn** om statistieken over het gebruik van informatie- en communicatietechnologieën te kunnen opstellen. Zoals de Autoriteit echter reeds eerder in haar advies heeft opgemerkt, zijn de gegevens die op grond van de artikelen 122 en 123 van de Telecomwet worden opgeslagen, zeer talrijk en gevarieerd en kunnen zij derhalve, zoals het Hof van Justitie meermaals heeft opgemerkt, *"informatie onthullen over een aanzienlijk aantal aspecten van het privéleven van de betrokkenen, waaronder gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, godsdienstige, levensbeschouwelijke, maatschappelijke of andere overtuigingen en gezondheidstoestand [...]. Uit deze gegevens, in hun geheel beschouwd, kunnen*

³⁴ In meerdere overwegingen van de verordeningen 2019/1700 en 2019/1952 wordt gewezen op het belang van betrouwbare statistieken om de overheden in staat te stellen verantwoordelijke beleidslijnen in te voeren. Zie bijvoorbeeld de eerste overweging van verordening 2019/1700: "Statistische gegevens en indicatoren vormen de ruggengraat van verantwoordelijk op feiten gebaseerd beleid. In het kader van de Europa 2020-strategie en het versterken van economisch bestuur spelen sociale indicatoren een wezenlijke rol bij de voorlichting over en ondersteuning van de belangrijkste prioriteiten van de Unie. Die prioriteiten hebben met name betrekking op inclusieve en duurzame groei en werkgelegenheid, sociale cohesie, de vermindering van armoede, ongelijkheden en sociale uitsluiting, de integratie van personen met een handicap, gelijke behandeling, en vaardigheden, mobiliteit en de digitale economie. Met name zijn sociale indicatoren nodig om een solide statistische basis te bieden voor de ontwikkeling van en het toezicht op het beleid dat door de Unie en de lidstaten wordt geïntroduceerd om die prioriteiten aan te pakken. Kwalitatief hoogwaardige sociale statistieken zijn noodzakelijk om de weerbaarheid van de Unie te vergroten, haar cohesiedoelstellingen te helpen bereiken en haar welvaartsniveaus te behouden. Solide gegevens zijn tevens van het grootste belang om zich te wapenen tegen misleidende informatie."

*zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. Aan de hand van deze gegevens kan het profiel van de betrokken personen worden bepaald, informatie die, wat het recht op bescherming van het privéleven betreft, even gevoelig is als de inhoud zelf van de communicaties.*³⁵

51. **Het verlenen van toegang aan het NIS tot alle verkeers- en lokalisatiegegevens** die door de operatoren worden bewaard ter uitvoering van de nieuwe artikelen 122 en 123 van de Telecomwet, **gaat verder dan wat noodzakelijk is om het NIS in staat te stellen het beoogde statistische doel te bereiken.** Overeenkomstig het evenredigheidsbeginsel en het beginsel van minimalisering van gegevens³⁶ **moet aan het NIS alleen toegang worden verleend tot de gegevens die noodzakelijk zijn voor de statistische doeleinden,** met name de productie van statistieken, overeenkomstig de bovengenoemde EU-verordeningen, over het gebruik van informatie- en communicatietechnologieën door de huishoudens en de ondernemingen.

52. Naar aanleiding van een verzoek om aanvullende inlichtingen heeft de afgevaardigde van de minister **de categorieën gegevens geïdentificeerd** die voor het NIS noodzakelijk zijn om zijn statistische doel te bereiken:

- " • Vast internet: het adres van een aansluiting -> De gegevens zijn nodig om de koppeling te kunnen maken met een huishouden en zo te bepalen of de leden van een huishouden toegang hebben tot vast internet.*
- Vast internet: de identiteit van de persoon (naam, voornaam en adres of het rijksregisternummer) of onderneming (naam en adres of KBO-nummer of btw-nummer) die het contract heeft afgesloten -> De gegevens zijn nodig om de koppeling te kunnen maken met een huishouden en zo te bepalen of de leden van een huishouden toegang hebben tot vast internet.*
- Vast internet: Informatie over het type verbinding op het vlak van de potentiële snelheid (bv. Viber, ...) -> De gegevens zijn nodig om bij nieuwe technologieën na te gaan welke profielen toegang hebben tot de nieuwe technologie en welke profielen uitgesloten zijn.*
- Mobiel internet: de identiteit van de persoon (naam- adres of het rijksregisternummer) of onderneming (naam- adres of KBO-nummer of btw-nummer) die het contract heeft afgesloten. -> De gegevens zijn nodig om de koppeling te kunnen maken met een*

³⁵ Zie bijvoorbeeld HvJEU, 8 april 2014, *gevoegde zaken C-293/12 en C-594/12, "Digital Rights Ireland et al."*, § 27; HvJEU, 21 december 2016, *gevoegde zaken C-203/15 en C-698/15, "Tele2 Sverige et al."*, § 99; HvJEU, 2 oktober 2020, *gevoegde zaken C-511/18, C-512/18 en C-520/18, "Quadrature du Net et al."*, § 117.

³⁶ Dit beginsel is vastgelegd in het Handvest van de grondrechten van de Europese Unie, de e-Privacyrichtlijn, de e-privacy-richtlijn en de wet van 4 juli 1962.

persoon en nadien huishouden en zo te bepalen of iemand van het gezin toegang heeft tot mobiel internet.

- *Informatie over de facturatie aan klanten: de identiteit van de persoon of de onderneming aan wie de factuur gericht is -> De gegevens zijn nodig om de koppeling te kunnen maken met de gezinnen die deelnamen aan het Huishoudbudgetonderzoek.*
- *Informatie over de facturatie aan klanten: Bedrag van de factuur, periode, de opdeling van de kostprijs per dienst (vast internet, mobiel internet, vaste telefoon, mobiele telefoon en digitale tv) -> De gegevens zijn nodig om de informatie van het Huishoudbudgetonderzoek te verrijken en zo een beter beeld te krijgen van de uitgaven van gezinnen voor Telecomdiensten."*

53. Het **nieuwe artikel 24sexies** van de wet van 4 juli 1962, ingevoerd door artikel 47 van het wetsontwerp, **moet dus worden gewijzigd om de categorieën van gegevens op te nemen waartoe het NIS toegang kan hebben** onder alle gegevens die de operatoren bewaren in uitvoering van de nieuwe artikelen 122 en 123 van de Telecomwet, met dien verstande dat deze gegevens relevant, adequaat en beperkt moeten zijn tot wat noodzakelijk is voor het nagestreefde doel.
54. Voorts merkt de Autoriteit op dat het voor het opstellen van statistieken over het gebruik van informatie- en communicatietechnologieën door de huishoudens en de ondernemingen **niet nodig is de gegevens van de gehele bevolking te verzamelen**. Om de beginselen van noodzakelijkheid en evenredigheid in acht te nemen, moet in het ontwerp worden bepaald dat **de verzameling beperkt moet blijven tot een representatieve steekproef van de bevolking**. Het **ontwerp moet** dienovereenkomstig **worden aangepast**.
55. Bovendien geeft het nieuwe artikel 24sexies van de wet van 4 juli 1962, ingevoerd bij artikel 47 van het wetsontwerp, het NIS de bevoegdheid om permanent toegang te hebben tot gegevens die bewaard worden door de telecomoperatoren. Op de vraag om de noodzaak van een dergelijke permanente toegang tot verkeers- en lokalisatiegegevens te rechtvaardigen, verklaarde de afgevaardigde van de minister: *"Het volstaat dat Statbel 2 keer per jaar de gegevens ontvangt. Deze frequentie is noodzakelijk omdat de ICT-enquête een jaarlijkse enquête is. De veldwerkperiode van de enquête loopt van januari van het jaar tot en met augustus. De resultaten dienen eind september aan Eurostat geleverd te worden. Om dit voor te bereiden wordt er in juni al een tussentijds bestand aangemaakt met de gegevens voor de periode januari tot en met april."*
56. Aangezien het voor het bereiken van het statistische doel voldoende is dat het NIS tweemaal per jaar toegang heeft tot de relevante verkeersgegevens, is het **ter uitvoering van de beginselen van noodzakelijkheid en evenredigheid** passend te bepalen dat **het NIS alleen op bepaalde**

tijdstippen van het jaar (en niet het hele jaar door) **toegang kan krijgen** tot de gegevens die door de telecomoperatoren worden bijgehouden. Op basis van de door de afgevaardigde van de minister verstrekte informatie zou de ontwerpbeplanning kunnen voorzien in de toegang tot gegevens tweemaal per jaar. De ontwerpbeplanning **moet in die zin worden aangepast**.

57. Concluderend benadrukt de Autoriteit dat, indien het nieuwe artikel 24^{sexies} van de wet van 4 juli 1962, ingevoerd bij artikel 47 van het wetsontwerp, zou worden gewijzigd overeenkomstig de hierboven gedane aanbevelingen, de ontwerpbeplanning zou zorgen voor een billijk evenwicht tussen de verschillende betrokken belangen en tegelijk een voldoende precies en voorzienbaar kader zou bieden voor de omstandigheden en voorwaarden waaronder het NIS toegang kan hebben tot de telecomgegevens.

E. Slotopmerking over de toekenning van nieuwe bevoegdheden aan de Gegevensbeschermingsautoriteit door het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens

58. **Op eigen initiatief**, en geenszins uitputtend, heeft de Autoriteit opgemerkt dat **de artikelen 19 en 34 van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens een nieuwe bevoegdheid aan de Autoriteit verlenen**.
59. Het nieuwe artikel 28/1, § 2 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, ingevoegd bij artikel 19 van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens, bepaalt het volgende:

"Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mogen de personeelsleden van het Instituut die niet in een strafrechtelijk kader optreden, van een operator eisen dat hij hen andere door de operator bewaarde metagegevens van elektronische communicatie verstrekt dan de gegevens betreffende de eindgebruiker of de abonnee.

Hij legt zijn met redenen omkleed verzoek vooraf voor goedkeuring voor aan de Gegevensbeschermingsautoriteit, behalve in een naar behoren gerechtvaardigd noodgeval. In een naar behoren gerechtvaardigd noodgeval deelt hij het naar de operator verzonden verzoek na deze verzending onverwijld mee aan de

Gegevensbeschermingsautoriteit. De Gegevensbeschermingsautoriteit voert daarna een controle uit."

60. De *in artikel 14, § 1, 3°, a) en g) tot i)*, van de wet van 17 januari 2003 opgesomde opdrachten zijn de volgende: " *het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:*

a) de wet van 13 juni 2005 betreffende de elektronische communicatie;

[...]

g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;

h) 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, met betrekking tot de sector digitale infrastructuren;

i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie"

61. Het nieuwe artikel 62, § 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, zoals gewijzigd bij artikel 34 van 19 van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens, bepaalt als volgt:

" Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e), van deze wet, kan het nationale CSIRT gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens als bedoeld in artikel 2, 9,1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie verkrijgen van een operator als bedoeld in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die deze gegevens bewaart

De doeleinden van voornoemde taken zijn:

- het voorkomen van ernstige bedreigingen voor de openbare veiligheid;*
- het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen;*
- het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.*

Indien het nationale CSIRT een operator een verzoek om gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.

Indien het nationale CSIRT een operator een verzoek om elektronische-communicatie metagegevens als bedoeld in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie die geen in het vorige lid bedoelde gegevens zijn, stuurt, moet dat verzoek vooraf worden gecontroleerd door de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017.

In dringende en naar behoren gemotiveerde gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het vorige lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het vorige lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.

De directeur van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om deze elektronische-communicatiegegevens te verwerken.

Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering”.

62. De taken waarvoor het *nationale CSIRT*, met name het CCB, metagegevens over elektronische communicatie kan verkrijgen, zijn de volgende:

- a) monitoren van incidenten op nationaal en internationaal niveau, met inbegrip van de verwerking van persoonsgegevens met betrekking tot het monitoren van deze incidenten;*
- b) ten behoeve van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;*
- c) reageren op incidenten;*
- d) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;*
- e) computerbeveiligingsproblemen opsporen, observeren en analyseren."*

63. De Autoriteit stelt allereerst vast dat de memorie van toelichting bij het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens geen uitleg of informatie bevat die het mogelijk maakt concreet te begrijpen waarom het nodig kan zijn dat het BIPT en het CCB toegang hebben tot ruwe metagegevens van elektronische communicatie. **Het is aan de wetgever om zich**

ervan te vergewissen dat het inderdaad noodzakelijk is dat deze instellingen toegang hebben tot de ruwe metagegevens over communicatie, door met name na te gaan of deze instellingen hun opdrachten niet kunnen vervullen indien zij geen toegang hebben tot de metagegevens over communicatie. De Autoriteit benadrukt in het bijzonder dat indien het mogelijk is dat het BIPT en/of het CCB hun opdrachten uitvoeren met behulp van geanonimiseerde of gepseudonimiseerde gegevens, in het ontwerp moet worden bepaald dat alleen geanonimiseerde of gepseudonimiseerde gegevens aan hen mogen worden doorgegeven³⁷. **Indien en voor zover het BIPT en/of het CCB een openbaredienstopdracht hebben om cyberaanvallen in real time op te sporen en te beëindigen** (wat kan inhouden dat bepaalde diensten of IP-adressen moeten worden geblokkeerd om bijvoorbeeld DDOS-aanvallen te stoppen, botnets uit te schakelen of een einde te maken aan phishing-pogingen), **begrijpt de Autoriteit echter dat het BIPT en/of het CCB toegang moeten kunnen krijgen tot ruwe metagegevens van elektronische communicatie**

64. In het licht van de door een dergelijke toegang veroorzaakte inmenging in het recht op respect voor de privacy, is de Autoriteit van mening dat **het van essentieel belang is een diepgaand parlementair debat te houden om de exacte contouren te definiëren van de bevoegdheden en opdrachten** van de politiediensten, de **gerechtelijke diensten**, de inlichtingendiensten, de militaire diensten of ook de administratieve autoriteiten die belast zijn met het opsporen en bestrijden van cyberaanvallen. De Autoriteit dringt erop aan dat in dit debat ook wordt ingegaan op de noodzakelijke beperkingen op de verdere verwerkingen (bijvoorbeeld door inlichtingendiensten of politiediensten) van metagegevens die zijn verzameld in het kader van de bestrijding van cybercriminaliteit.
65. Vervolgens merkt de Autoriteit op dat de vereiste van voorzienbaarheid, in combinatie met het principe van gegevensminimalisering zoals vastgelegd in artikel 5.1. c) van de AVG, vereist dat de ontwerpbepalingen **nauwkeurig afbakenen tot welke categorieën van gegevens het BIPT of het CCB toegang kunnen hebben om welke opdrachten te kunnen vervullen**. Met andere woorden, de ontwerpbepalingen moeten voor elke opdracht van het BIPT en het CCB de categorieën van gegevens identificeren waartoe deze instellingen toegang moeten hebben om de hun toevertrouwde openbaredienstopdrachten te kunnen vervullen, rekening houdend met het feit dat deze categorieën van gegevens *"toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt"*.

³⁷ De Autoriteit wijst er echter op dat het bijzonder moeilijk kan zijn om metagegevens van elektronische communicatie daadwerkelijk te anonimiseren of zelfs te pseudonimiseren. Het blijkt namelijk heel goed mogelijk, en zelfs heel gemakkelijk, om personen opnieuw te identificeren aan de hand van een reeks geanonimiseerde metagegevens van elektronische communicatie. Zie Ana-Maria Crețu, Federico Monti, Stefano Marrone, Xiaowen Dong, Michael Bronstein, Yves-Alexandre de Montjoye, "Interaction data are identifiable even across long periods of time", Nature Communications, 25 januari 2022

66. Gezien de ernst van de risico's op misbruik, is de Autoriteit bovendien, in overeenstemming met de Europese rechtspraak, van mening dat de toegangen tot de metagegevens van communicatie die plaatsvinden in het kader van opdrachten **die het nemen van dwangbesluiten** ten aanzien van betrokkenen **impliceren** of die een **massale verzameling** van metagegevens van elektronische communicatie **impliceren, moeten worden onderworpen aan een onafhankelijke controle** door een instantie die beschikt over **toereikende technische expertise**.
67. Voor de opdrachten van het BIPT en het CCB **die geen dwangbesluit impliceren** ten aanzien van betrokkenen en **die geen massale verzameling** van metagegevens van elektronische communicatie **impliceren, komt het daarentegen toe aan de wetgever om deze toegang passend te regelen** door die te beperken tot geanonimiseerde gegevens, of ook gepseudonimiseerde gegevens, en daarbij het gebruik van de pseudonimiseringssleutel te beveiligen en te voorzien in alle andere passende maatregelen³⁸, liever dan te voorzien in een systeem van voorafgaande toestemming.
68. Het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens kent aan de Autoriteit de bevoegdheid toe om op voorhand controle uit te oefenen op elke mededeling van communicatiemetagegevens aan het BIPT en het CCB in het kader van hun opdrachten die dwangbesluiten ten aanzien van de betrokkenen impliceren. Hierover wenst de Autoriteit **meerdere opmerkingen** te formuleren:
69. In de eerste plaats merkt de Autoriteit op dat het nieuwe artikel 62 van de wet van 7 april 2019, ingevoerd door het herziene wetsvoorstel over het verzamelen en bewaren van telecomgegevens, bepaalt dat de toegang van het CCB tot verkeers- en locatiegegevens onder meer het volgende doel nastreeft: *"het voorkomen, onderzoeken en opsporen van strafbare feiten die online of via een elektronisch communicatienetwerk of een elektronische communicatiedienst zijn gepleegd, met inbegrip van strafbare feiten die verband houden met zware criminaliteit"*. In dit verband **vraagt de Autoriteit zich af wat de samenhang is van het feit dat zij wordt belast met de opdracht van voorafgaande toetsing** ter waarborging van de relevantie, de noodzaak en de evenredigheid van de communicatie van verkeers- en lokalisatiegegevens aan het CCB, terwijl voor de communicatie van verkeers- en lokalisatiegegevens aan alle andere categorieën overheidsinstanties die belast zijn met een opdracht die het nemen van een dwangbesluit tegen een persoon impliceert, de voorafgaande toetsing van de communicatie van metagegevens inzake telecommunicatie wordt verricht door de onderzoeksrechter.
70. De Autoriteit vestigt vervolgens de aandacht op het feit **dat zij momenteel noch over de nodige technische deskundigheid, noch over de noodzakelijke middelen beschikt om deze nieuwe**

³⁸ De Autoriteit is zich echter bewust van de moeilijkheid van het anonimiseren van metagegevens (cf. supra).

opdracht effectief uit te voeren. Welnu, de onafhankelijke toetsing vormt immers slechts dan een passende garantie voor de betrokkenen als ze wordt uitgeoefend door een autoriteit die beschikt over toereikende technische deskundigheid. Als dat niet zo is, dient de voorafgaande toetsing nergens toe. Indien de auteur van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens volhardt in zijn voornemen om een opdracht van voorafgaande toetsing toe te vertrouwen aan de Autoriteit, moet hij verzekeren dat ze over de nodige extra middelen zal beschikken voor de uitoefening van deze opdracht, waarvoor nieuwe profielen moeten worden aangeworven die beschikken over een heel specifieke technische en juridische deskundigheid, die niet aanwezig is bij de personeelsleden van de Autoriteit. **In deze omstandigheden vraagt de Autoriteit zich af of er geen instantie bestaat die beter toegerust en gekwalificeerd is om een dergelijke toetsing uit te voeren, dan wel of er geen nieuwe gespecialiseerde instelling moet worden opgericht met het oog op de uitoefening van een dergelijke toetsing.**

71. Deze vraag **is des te prangender** omdat het feit dat aan de Autoriteit een opdracht van voorafgaande toetsing wordt toevertrouwd, na afloop waarvan zij de mededeling van de metagegevens van telecommunicatie moet toestaan of weigeren, **afbreuk dreigt te doen aan de vereiste van onpartijdigheid die aan de Autoriteit wordt opgelegd**, wat onder meer in overweging 129 van de AVG in herinnering wordt gebracht³⁹. Ter herinnering: het beginsel van onpartijdigheid vereist niet alleen dat de Autoriteit onpartijdig handelt, dat wil zeggen zonder 'vooringenomenheid' ('subjectieve' onpartijdigheid), maar ook dat zij onpartijdig lijkt te handelen ('objectieve' onpartijdigheid)⁴⁰. **Objectieve onpartijdigheid vereist dat de context waarin de Autoriteit haar bevoegdheid uitoefent, geen aanleiding geeft tot een gewettigde vrees voor partijdigheid.** Door de Autoriteit te belasten met de voorafgaande toetsing – en de voorafgaande toelating – van de communicatie van metagegevens over telecommunicatie aan het BIPT en het CCB, dreigt de wetgever de onpartijdigheid van de Autoriteit in haar objectieve dimensie te ondermijnen. De personen die betrokken zijn bij een communicatie van metagegevens over telecommunicatie aan het CCB of het BIPT, moeten krachtens artikel 77 van de AVG het recht hebben een klacht in te dienen bij een toezichthoudende autoriteit *"indien hij van mening is dat de verwerking van hem betreffende persoonsgegevens inbreuk maakt op [de AVG]"*. Zodra de Autoriteit echter toestemming heeft gegeven voor de communicatie van gegevens voordat deze is uitgevoerd, kan de betrokkene terecht twijfelen aan de onpartijdigheid van de Autoriteit indien zij a posteriori via haar inspectiedienst of haar Geschillenkamer controle zou moeten uitoefenen op de bedoelde communicatie⁴¹. Deze twijfel over het vermogen van de Autoriteit om haar dwingende bevoegdheden onpartijdig uit te oefenen wanneer

³⁹³⁹ "De bevoegdheden van de toezichthoudende autoriteiten moeten overeenkomstig passende in het Unierecht en het lidstatelijke recht bepaalde procedurele waarborgen, onpartijdig, behoorlijk en binnen een redelijke termijn worden uitgeoefend."

⁴⁰ Dit is een toepassing van de regel *"Justice must not only be done, it must also be seen to be done"*.

⁴¹ In dezelfde geest zou het ook lastig zijn om de afdeling Wetgeving van de Raad van State de bevoegdheid te geven om vooraf toestemming te geven voor bindende bestuursrechtelijke beslissingen, terwijl zijn afdeling administratieve geschillen later, in een fase van een geding, kan worden verzocht de geldigheid van dergelijke beslissingen te beoordelen.

zij eerder toestemming heeft gegeven voor de communicatie van gegevens, zal des te sterker zijn na de hervorming van de Autoriteit, aangezien het voorontwerp van wet tot wijziging van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit de collegiale werking van de Autoriteit en haar verschillende organen wil versterken.

72. In ieder geval, indien de auteur van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens ondanks de zojuist geformuleerde overwegingen en bedenkingen de opdracht van voorafgaande toetsing aan de Autoriteit wil blijven toevertrouwen, **benadrukt de Autoriteit dat hij moet verzekeren dat de Autoriteit de haar toevertrouwde nieuwe opdrachten met de vereiste doeltreffendheid kan uitvoeren**, zo niet, dan zou de Belgische reglementering niet in overeenstemming zijn met de e-Privacyrichtlijn, zoals uitgelegd door het HvJEU.
73. Tot slot vestigt de Autoriteit de aandacht op het feit dat de bepalingen van het ontwerp aan de Europese Commissie moeten worden gemeld ter uitvoering van artikel 51.4 van de AVG.

OM DEZE REDENEN,

Is de Autoriteit van oordeel dat de volgende wijzigingen moeten worden aangebracht aan het wetsontwerp:

- Bepalen dat de metagegevens van elektronische communicatie die onrechtmatig verkregen zijn, niet mogen worden gebruikt tegen de betrokkene in het kader van een procedure die impliceert dat ten aanzien van de betrokkene een dwangbesluit wordt genomen (overw. 10, 19, 35).
- Invoegen van een verplichting ten laste van de BMA, de FOD Economie en het NIS om jaarlijks statistieken te publiceren over (1) het aantal toegangen dat hun werd toegestaan, (2) het aantal metagegevens waartoe zij toegang hebben gehad, (3) het aantal personen dat bij die toegang betrokken was, (4) de impact van die toegangen op de uitoefening van hun opdrachten (overw. 12).
- Alle dubbelzinnigheden wegwerken met betrekking tot het feit dat de IP-adressen enkel aan de ambtenaren van de EI mogen worden verstrekt met het oog op het onderzoeken en vaststellen van inbreuken op het WER van niveau 5 of 6 (overw. 30).
- Opnemen van het concrete statistische doel waarvoor het NIS toegang kan vragen tot de door de telecomoperatoren bewaarde gegevens zoals bedoeld in het nieuwe artikel 127/1, § 2 van de Telecomwet (overw. 44).

- Opnemen van categorieën gegevens waartoe het NIS toegang kan hebben, met dien verstande dat deze gegevens relevant, adequaat en beperkt moeten zijn tot wat noodzakelijk is voor het concrete nagestreefde statistische doel (overw. 50-53).
- Specificeren dat, om statistieken op te stellen over het gebruik van informatie- en communicatietechnologie door de huishoudens en de ondernemingen, het NIS enkel toegang mag hebben tot de relevante metagegevens van een representatieve steekproef van de bevolking (en niet van de gehele bevolking) (overw. 54).
- Bepalen dat het NIS alleen op bepaalde tijdstippen van het jaar (en niet het hele jaar door) toegang kan krijgen tot de gegevens van de telecomoperatoren (overw. 55-56).

Daarnaast vestigt de Autoriteit de aandacht op de volgende elementen:

- De herziene versie van het wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens, waarin de voorwaarden worden vastgesteld waaronder de operatoren verkeers- en lokalisatiegegevens moeten (of mogen) bewaren, moet in overeenstemming zijn met de e-Privacyrichtlijn, anders kan de toegang tot dergelijke gegevens niet worden geacht in overeenstemming te zijn met die richtlijn (overw. 6-8).
- De identificatie van een persoon aan de hand van een telefoonnummer of IP-adres maakt het mogelijk de persoon te identificeren die op de betrokken elektronische-communicatiedienst is geabonneerd, maar deze persoon zal niet noodzakelijkerwijs overeenkomen met de persoon die het strafbare feit heeft gepleegd of daarbij betrokken was (overw. 26).
- Wanneer een onderzoeksrechter een verzoek om toegang tot de door de telecomoperatoren bewaarde gegevens ontvangt, is hij enkel verplicht toegang te verlenen tot die gegevens indien er, gelet op de feiten, een geheel van overeenstemmende en ernstige aanwijzingen bestaat dat de opgevraagde persoonsgegevens het onderzoek naar en de vaststelling van strafbare feiten mogelijk zouden maken of zouden bespoedigen (overw. 33).
- De auteur van het wetsontwerp moet ervoor zorgen dat het regelgevingskader waarborgt dat de personen op wie de mededeling van hun gegevens betrekking heeft, naar behoren van deze mededeling in kennis worden gesteld zodra deze informatie het door deze autoriteiten verrichte onderzoek niet langer in gevaar kan brengen (overw. 34).

- De auteur van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens moet nagaan of het echt wel nodig is dat het BIPT en het CCB toegang hebben tot de verkeers- en lokalisatiegegevens die door de telecomoperatoren worden bewaard, door met name na te gaan of deze instellingen hun opdrachten niet kunnen vervullen indien zij geen toegang hebben tot deze gegevens (overw. 63).
- Meer fundamenteel is een diepgaand parlementair debat nodig om de precieze bevoegdheden en opdrachten af te bakenen van de verschillende instellingen (politie, inlichtingendiensten, defensie, justitie, administratieve autoriteiten) die betrokken zijn bij de bestrijding van cybercriminaliteit, vooral omdat de maatregelen die kunnen worden genomen in het kader van de strijd tegen cybercriminaliteit in zeer grote mate interfereren met het recht op privacy en het recht op bescherming van de persoonsgegevens van de burgers (overw. 64).
- Indien nodig moet de auteur van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens voor elke opdracht van het BIPT en het CCB de categorieën van gegevens identificeren waartoe deze instellingen toegang moeten hebben om de hun toevertrouwde openbaredienstopdrachten te kunnen vervullen, rekening houdend met het feit dat deze categorieën van gegevens *"toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt"* (overw. 65).
- De Autoriteit is van mening dat het voor de opdrachten van het BIPT en het CCB die niet inhouden dat 'massaal' metagegevens van elektronische communicatie worden verzameld, noch dat een dwangbesluit wordt genomen ten aanzien van betrokkenen, daarentegen toekomt aan de wetgever om deze toegang passend te regelen door die te beperken tot geanonimiseerde gegevens, of ook gepseudonimiseerde gegevens, en daarbij het gebruik van de pseudonimiseringssleutel te beveiligen en te voorzien in alle andere passende maatregelen, liever dan te voorzien in een systeem van voorafgaande toestemming (overw. 67).
- De Autoriteit vraagt zich af wat de samenhang is van het feit dat zij wordt belast met de taak van voorafgaande toetsing ter waarborging van de relevantie, de noodzaak en de evenredigheid van de communicatie van verkeers- en lokalisatiegegevens aan het CCB, terwijl voor de communicatie van verkeers- en lokalisatiegegevens aan alle andere categorieën overheidsinstanties die belast zijn met een opdracht die het nemen van een dwangbesluit tegen een persoon impliceert, de voorafgaande toetsing van de communicatie van metagegevens inzake telecommunicatie wordt verricht door de onderzoeksrechter (overw. 69).
- De Autoriteit vestigt de aandacht op het feit dat zij momenteel noch over de nodige technische deskundigheid, noch over de noodzakelijke middelen beschikt om doeltreffend controle uit te

oefenen op de relevantie, de noodzaak en de evenredigheid van de mededelingen van verkeers- en lokalisatiegegevens aan instelling die belast zijn met het waken over de veiligheid van de netwerken (overw. 70). Ze wijst er bovendien op dat e uitoefening van een dergelijke opdracht van voorafgaande toestemming dreigt de aan haar opgelegde vereiste van onpartijdigheid te ondermijnen (overw. 71). In deze omstandigheden vraagt de Autoriteit zich af of er geen instantie bestaat die beter toegerust en gekwalificeerd is om een dergelijke toetsing uit te voeren, dan wel of er geen instelling moet worden opgericht voor de uitoefening van een dergelijke toetsing (overw. 70).

- Als de auteur van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens volhardt in de wens om de opdracht van voorafgaande toetsing toe te vertrouwen aan de Autoriteit, ondanks de net geformuleerde overwegingen en bedenkingen, moet hij zich ervan vergewissen, voordat deze nieuwe opdracht aan haar wordt toevertrouwd, dat ze over de nodige extra middelen zal beschikken voor de uitoefening van deze extra opdracht (overw. 72).
- De artikelen 19 en 34 van het herziene wetsontwerp betreffende het verzamelen en bewaren van telecomgegevens moeten aan de Europese Commissie worden gemeld ter uitvoering van artikel 51.4 van de AVG (overw. 73).

Voor het Kenniscentrum,

(get.) Rita Van Nuffelen - Verantwoordelijke a.i. van het Kenniscentrum