Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 66/2022 van 1 april 2022

Betreft: Adviesaanvraag over 18 amendementen tot wijziging van het 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 (CO-A-2022-057)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),
Aanwezig : de heer Bart Preneel.

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

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

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

Gelet op de adviesaanvraag van de heer Vincent Van Quickenborne, vicepremier en minister van Justitie en bevoegd voor de Noordzee, ontvangen op 1 maart 2022;

Brengt op 1 april 2022 het volgend advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De vice-eersteminister en minister van Justitie, en bevoegd voor de Noodzee vroeg het advies van de Autoriteit over **18 amendementen tot wijziging van het 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 "de amendementen").

2. Het wetsontwerp betreffende het verzamelen en bewaren van identificatiegegevens en metagegevens in de sector elektronische communicatie en de verstrekking ervan aan de autoriteiten (hierna **"het ontwerp van herstelwet van de wet dataretentie**" of "**ontwerp van herstelwet**") geeft gevolg aan de vernietiging door het Gronddwettelijk Hof, in zijn arrest nr. 57/2021 van 22 april 2021 *«van de artikelen 2 b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie*(hierna "**de wet van 29 mei 2016**") »).

3. In de brief die de aanvrager stuurde naar de Autoriteit werd eraan herinnerd dat deze wet van 29 mei 2016 bepaalde (de Autoriteit vertaalt): «*de verplichting voor aanbieders van telefoondiensten, met inbegrip van internetdiensten, internettoegang en e-mail via internet aan het publiek (ongeacht of zij al dan niet bij het BIPT aangemelde operatoren zijn) om bepaalde categorieën locatie- en verkeersgegevens gedurende twaalf maanden te bewaren, hoofdzakelijk om deze gegevens beschikbaar te stellen voor rechtshandhavingsdoeleinden (strafrechtelijke onderzoeken) of voor de uitvoering van de taken van inlichtingen- en veiligheidsdiensten*» Deze wet uit 2016 legde dus een algemene en ongedifferentieerde bewaringsplicht op voor bepaalde verkeers- en locatiegegevens, maar had geen betrekking op de inhoud van de communicatie. Zij is door het Grondwettelijk Hof nietig verklaard omdat zij in strijd is met artikel 15 van 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 (hierna "de e-privacyrichtlijn" genoemd), gelezen in het licht van de artikelen 7 en 8, alsook artikel 52, §1, van het Handvest van de grondrechten van de Europese Unie, in samenhang met de artikelen 10 en 11 van de Grondwet. De vernietiging door het Grondwettelijk Hof is grotendeels ingegeven door een verwijzing naar het arrest dat het Hof van Justitie van de Europese Unie (hierna "het HvJEU") heeft gewezen naar aanleiding van de prejudiciële vragen die onder meer door het Grondwettelijk Hof zijn gesteld over de interpretatie die moet worden gegeven aan artikel 15 van de e-privacyrichtlijn[1].

[1] HJEU, arrest van 6 oktober 2020, samengevoegde zaken C-511/18, C-512/18 en C-520/18,(de zogenaamde zaak "La Quadrature du Net"). Dit arrest van het HvJEU is onder meer gewezen naar aanleiding van de prejudiciële vragen die het Grondwettelijk Hof heeft gesteld in zijn arrest nr. 96/2018 van 19 juli 2018.

4. Naar aanleiding van deze uitspraak **heeft de regering een ontwerp van wet om de dataretentiewet te herstellen, voorbereid waarover de Autoriteit zich uitsprak in haar advies nr. 108/2021 van 28 juni 2021**.

5. Op 18 november 2021 heeft het Grondwettelijk Hof «*artikel 2 de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst nietig verklaard, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen*». In dit arrest 158/2021 oordeelde het Grondwettelijk Hof inderdaad *dat «artikel 127 van de wet van 13 juni 2005, zoals gewijzigd bij artikel 2 van de bestreden wet, het wettigheidsbeginsel gewaarborgd door artikel 22 van de Grondwet schendt, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen* »[2]. Met andere woorden, **het Grondwettelijk Hof** herinnert er in dit arrest aan dat het in artikel 22 van de Grondwet verankerde **legaliteitsbeginsel vereist dat de wetgever zelf bepaalt welke identificatiegegevens en -documenten** door de operatoren **moeten worden bijgehouden**, aangezien deze identificatiegegevens en -documenten een essentieel element vormen van de verwerking van persoonsgegevens.

6. Ter herinnering: het in artikel 22 van de Grondwet verankerde legaliteitsbeginsel waarborgt «*elke rechtzoekende dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het legaliteitsheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld*». De **identificatiegegevens en -documenten** die de telecomoperatoren moeten bijhouden, vormen volgens het Grondwettelijk Hof een **essentieel element** dat **door de wetgever zelf moet worden bepaald**, en niet aan de uitvoerende macht kan worden gedelegeerd.

7. Als gevolg van dit arrest 158/2021 is de regering van mening dat sommige bepalingen van de herstelwet moesten worden herzien. De **voor advies ingediende amendementen beogen onder meer gevolg te geven aan dit arrest** en ervoor te zorgen dat de bepalingen van 13 juni 2005 betreffende elektronische communicatie (hierna "de telecomwet"), zoals zij door de herstelwet zullen worden gewijzigd, die de operatoren verplichten bepaalde gegevens te bewaren (hetzij de abonneegegevens, identificatiegegevens of verkeers- of locatiegegevens), voldoen aan het beginsel van formele wettigheid.

[2] Overweging nr. B.9.1 van het arrest.

8. Hoewel het arrest nr. 158/2021 van het Grondwettelijk Hof enkel betrekking heeft op artikel 127 van de telecomwet, blijkt uit de analyse van de regering dat ook andere bepalingen, met name de artikelen 126 en 126/1 van de telecomwet, moeten worden herzien om een lijst op te stellen van de gegevens die door de operatoren moeten worden bijgehouden.

9. Amendement 1 strekt dus tot **vervanging van artikel 126** van de telecommunicatiewet, dat de operatoren verplicht de **abonneegegevens en de technische gegevens** te bewaren die nodig zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst **te identificeren**, indien en voor zover de operator dergelijke gegevens verwerkt of genereert. In de nieuwe versie van artikel 126 worden de gegevens opgesomd die door de operatoren moeten worden bewaard voor zover zij deze verwerken of genereren in het kader van het aanbieden van elektronische communicatienetwerken of elektronische communicatiediensten.

10. De **amendementen 2 en 3** strekken ertoe in de telecomwet de metagegevens betreffende elektronische communicatie, met inbegrip van de metagegevens van mislukte gesprekken, op te nemen waarop de bewaarplicht van het **nieuwe artikel 126/1**, dat door het ontwerp van herstelwet in de telecomwet zal worden ingevoegd, van toepassing is. Deze metagegevens over elektronische communicatie zullen worden opgesomd in **een nieuw artikel 126/2** van de telecomwet.

11. **Amendement 4** strekt ertoe **artikel 145** van de telecomwet aan te passen zodat niet-naleving van het koninklijk besluit tot uitvoering van artikel 126/2 wordt bestraft met de strafrechtelijke geldboete waarin artikel 145 voorziet. **Amendement nr. 5** strekt ertoe een artikel 39 toe te voegen aan het ontwerp van herstelwet om operatoren een termijn van één jaar te geven om "nieuwe gegevens" te bewaren, d.w.z. gegevens bedoeld in de nieuwe artikelen 126 en 126/2 van de telecomwet en die niet voorzien zijn in het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

12. **Amendement nr. 6** strekt tot vervanging van **artikel 127** van de telecomwet, dat de operatoren verplicht **hun abonnees te identificeren door middel van een methode voor directe identificatie** (die in beginsel moet worden gebruikt voor betaalde elektronische communicatiediensten) of een van de daarin genoemde **methoden voor indirecte identificatie** (die moeten worden gebruikt voor gratis elektronische communicatiediensten en die in bepaalde gevallen ook moeten worden gebruikt voor betaalde elektronische communicatiediensten).

13. **Amendement nr.7** heeft tot doel een nieuw **artikel 127/4** in de telecomwet in te voegen, dat een verbod overneemt dat voordien in artikel 127, § 2, van de Telecomwet was opgenomen. **Amendement nr. 8** strekt ertoe **artikel 145** van de telecomwet aan te passen om ervoor te zorgen dat niet-naleving van het nieuwe artikel 127/4 van de telecomwet (ingevoegd bij amendement nr. 7)

wordt bestraft met een strafrechtelijke boete. **Amendement nr. 9** waarbij een artikel 40 in het ontwerp van herstelwet wordt ingevoegd, heeft tot doel (1) te verduidelijken dat de wijzigingen in artikel 127 van de telecomwet alleen van toepassing zullen zijn op contracten die na de inwerkingtreding van de wet worden gesloten, (2) de operatoren 24 maanden de tijd te geven voordat zij alle in het nieuwe artikel 127 opgesomde identiteitsdocumenten moeten aanvaarden (deze termijn moet hen in staat stellen hun systemen aan te passen) en (3) de operatoren 24 maanden de tijd te geven voordat zij de nieuwe " minimale gegevens" moeten verzamelen die zij krachtens het nieuwe artikel 127 moeten verzamelen.

14. De **amendementen 10 tot en met 15** hebben tot doel de wet van 17 januari 2003 betreffende het statuut van de regulator van de Belgische post- en telecommunicatiesector (hierna "de BIPT-wet") te wijzigen om de voorwaarden vast te stellen waaronder **het BIPT toegang kan hebben tot de door de operatoren opgeslagen identificatie-, verkeers- en locatiegegevens.**

15. Een ongenummerd amendement - maar laten we het identificeren als **amendement nr. 16** - heeft tot doel **artikel 46bis van het Wetboek van Strafvordering** (hierna " WSV.") te wijzigen., teneinde de Procureur des Konings uitdrukkelijk de bevoegdheid te verlenen om, ter verkrijging van de identificatie van de abonnee of de eindgebruiker van een elektronische-communicatiedienst, de medewerking van banken en financiële instellingen te vorderen (op basis van de referentie van een eerder aan hem meegedeelde elektronische-banktransactie), gesloten centra of woonunits (voor buitenlanders) (op basis van de gegevens van het centrum of de plaats van verblijf waar het abonnement van de abonnee op een mobiele elektronische-communicatiedienst is genomen en die hem eerder zijn meegedeeld), andere rechtspersonen die zich namens en voor rekening van natuurlijke personen abonneren op of zich inschrijven voor een elektronische-communicatiedienst (op basis van de gegevens die hun eerder door een operator zijn meegedeeld)

16. Een ongenummerd amendement - maar laten we het identificeren als **amendement nr. 17** - heeft tot doel **artikel 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 (hierna "de wet van 24 januari 1977") te wijzigen om de inspectiedienst Consumentenproducten in staat te stellen de medewerking van banken en financiële instellingen te vragen, op basis van de referentie van een elektronische transactie die vooraf door een operator is meegedeeld, zodat de inspectiedienst de betrokken persoon kan identificeren.

17. Een ongenummerd amendement - maar laten we het identificeren als **amendement nr 18** - heeft tot doel **artikel 81 van de wet van 2 augustus 2002** betreffende het toezicht op de financiële sector en de financiële diensten (hierna "de wet van 2 augustus 2002") te wijzigen om de auditeur (of substituut-auditeur) van de Autoriteit voor Financiële Diensten en Markten (hierna "de FSMA") in staat

te stellen een verzoek in te dienen, om de identificatie van de abonnee of de eindgebruiker van de dienst te verkrijgen, de medewerking van banken en financiële instellingen (op basis van de referentie van een eerder aan hem meegedeelde elektronische bankverrichting), gesloten centra of plaatsen van verblijf (voor buitenlanders) (op basis van de gegevens van het centrum of de plaats van verblijf waar het abonnement van de abonnee op een mobiele elektronische-communicatiedienst is genomen en die hem eerder zijn meegedeeld), andere rechtspersonen die zich namens en voor rekening van natuurlijke personen abonneren op of inschrijven voor een elektronische-communicatiedienst (op basis van de gegevens die hen eerder door een operator zijn meegedeeld).

18. De aanvrager verzocht de Autoriteit deze wijzigingen met spoed te behandelen. De Autoriteit wenst te benadrukken dat zij, gezien de aanzienlijke gevolgen van de wijzigingen voor de rechten en vrijheden van alle personen die in België wonen die gebruik maken van elektronische communicatie, d.w.z. bijna de gehele bevolking, **onaanvaardbaar acht dat zij noch over de tijd noch over de middelen beschikt om de zaak in de best mogelijke omstandigheden te analyseren**. Bij wijze van uitzondering brengt de Autoriteit, ondanks haar ontoereikende middelen in verhouding tot haar werklast[3], **haar advies zo spoedig mogelijk uit.** Zij verzoekt de aanvrager in de toekomst te anticiperen op dergelijke adviesaanvragen die van grote invloed zijn op de rechten en vrijheden van de burgers.

19. Alvorens de voor advies voorgelegde amendementen te onderzoeken in het licht van het recht op bescherming van persoonsgegevens, herhaalt de Autoriteit dat in haar advies **nr. 108/2021,** waarin zij **talrijke opmerkingen** had, waarvan sommige fundamenteel, over het ontwerp van herstelwet *dataretentie*. De Autoriteit dringt erop aan dat het ontwerp van **herstelwet daadwerkelijk de perspectiefwijziging doorvoert** die de rechtspraak van het HJEU en het Grondwettelijk Hof oplegt en dat het daarom geen nieuwe maatregelen inzake de bewaring van verkeers- en locatiegegevens kan opleggen die zouden leiden tot de juridische of de facto herinvoering van verplichtingen om verkeers- of locatiegegevens te bewaren van alle of een te groot deel van de gebruikers van elektronische-communicatiemiddelen in België. In haar advies nr. 108/2021 merkte de Autoriteit evenwel op dat het wetsontwerp dat haar voor advies was voorgelegd, dit perspectief niet volledig veranderde, aangezien het de bedoeling was nieuwe maatregelen op te leggen voor de bewaring van verkeers- en locatiegegevens (ter bestrijding van fraude, kwaadwillig gebruik van het netwerk en ter waarborging van de netwerkbeveiliging), hetgeen zou kunnen leiden tot de de facto herinvoering van algemene en ongedifferentieerde verplichtingen inzake gegevensbewaring. **Tenzij het ontwerp van herstelwet grondig wordt herzien om ervoor te zorgen dat het de vereiste**

[3] In dit verband wijst de Autoriteit erop, zoals zij reeds heeft gedaan in de bijlage bij het advies over het wetsontwerp tot wijziging van de GBA-wet, dat **de werklast van het Kenniscentrum de afgelopen jaren meer dan verdrievoudigd is** (75 adviezen in 2017 en 249 in 2021), **terwijl de personele middelen die aan het Kenniscentrum zijn toegewezen, zijn afgenomen** (in 2018 werden 13 juristen ingezet voor het opstellen van adviezen, terwijl deze taak thans door 8 juristen wordt vervuld). Begin april 2022 had het kenniscentrum al 65 adviezen uitgebracht; dit voorspelt een verdere exponentiële toename van de werklast voor dit jaar 2022.

perspectiefwijzigng brengt, zou zowel het bewaren van dergelijke verkeers- en locatiegegevens door operatoren als de mededeling ervan aan 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. Een nieuwe nietigverklaring van de herstelwet door het Grondwettelijk Hof zou het vertrouwen van de burgers in de democratische instellingen ernstig kunnen ondermijnen.

20. **De Autoriteit dringt erop aan dat de wetgever bij de goedkeuring van het ontwerp van herstelwet de vereisten van het recht op bescherming van persoonsgegevens in acht neemt. Voor alle aspecten die niet in voorliggend advies zijn besproken, verwijst de Autoriteit naar haar advies 108/2021.** Overigens merkt de Autoriteit nu reeds op dat zij in beginsel alleen opmerkingen zal maken over de amendementen die haar voor advies zijn voorgelegd voor zover deze nodig lijken in het licht van de nieuwe elementen die deze amendementen doorvoeren en de motivering daarvan.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

21. De Autoriteit zal de **amendementen 1, 2, 3, 6, 7, 12, 15, 16, 17 en 18** hieronder behandelen, aangezien de overige amendementen geen opmerkingen behoeven wat betreft het recht op bescherming van persoonsgegevens.

22. Alvorens deze amendementen in detail te bestuderen in het licht van de vereisten die voortvloeien uit het recht op bescherming van persoonsgegevens, zoals vastgelegd in artikel 22 van de Grondwet, de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, de e-privacyrichtlijn en de AVG, wenst de Autoriteit evenwel een **inleidende opmerking** te maken over de uitbreiding van het toepassingsgebied van de gegevensbewaring en de verplichting om abonnees en eindgebruikers te identificeren.

A. Voorafgaande opmerking over de uitbreiding van het toepassingsgebied van de gegevensbewaring en de verplichting om abonnees en eindgebruikers te identificeren

23. Door de omzetting van het Europees Wetboek voor elektronische communicatie (hierna "EWEC") in de telecomwet[4], **heeft de wetgever onder meer de begrippen «*operator*»[5] en «*elektronische-communicatiediensten* »[6]" geherdefinieerd,** die worden gebruikt om het

[4] Deze omzetting vond plaats door de aanneming van de wet van 21 december 2021 tot omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie.
[5] Dit begrip wordt gedefinieerd «*als persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt*» (artikel 2, 11° van de telecomwet)
[6] Dit begrip wordt gedefinieerd als «*een gewoonlijk tegen vergoeding via elektronische-communicatienetwerken aangeboden dienst, die, met uitzondering van diensten waarbij met behulp van elektronische-communicatienetwerken en -diensten*

persoonlijke toepassingsgebied te bepalen van de aan operatoren opgelegde verplichtingen om verkeers- en locatiegegevens van abonnees te bewaren en de verplichting om abonnees en eindgebruikers van elektronische-communicatiediensten te identificeren. Zoals de Autoriteit reeds in haar advies nr. 108/2021 heeft opgemerkt, leiden **deze nieuwe definities tot een aanzienlijke uitbreiding van de reikwijdte van de verplichtingen om gegevens te bewaren en abonnees en eindgebruikers te identificeren**. Met de omzetting van het EWEC in de telecomwet zijn bedrijven die over-the-top elektronische communicatiediensten aanbieden, zoals Voice over IP-diensten, berichtendiensten (bv. : WhatsApp, Signal, Telegram, Facebook Messenger), of online e-maildiensten (bv. : Gmail of Hotmail), onderworpen aan gegevensbewaringsverplichtingen en moeten zij hun abonnees of eindgebruikers identificeren. Ook de ondernemingen die instaan voor het aanbieden van «*diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt* »[7] - het gaat om diensten in verband met het internet van de dingen - moeten nu worden beschouwd als operatoren die onderworpen zijn aan gegevensbewaringsverplichtingen en de verplichting om hun abonnees en eindgebruikers te identificeren.

24. De nieuwe definities van "operator" en "elektronische communicatiedienst", in het bijzonder gekoppeld aan de identificatieplicht die wordt opgelegd door de nieuwe artikelen 126 en 127 van de telecomwet (ingevoerd bij Amendementen nrs. 1 en 6), **maken het onmogelijk - of op zijn minst zeer moeilijk - om anoniem te corresponderen op het internet.** Bovendien merkt de Autoriteit op met betrekking tot de " OTT -berichtendiensten (zoals Signal of WhatsApp) dat het verzamelen en bewaren van IP-adressen die aan de bron van de verbinding worden toegewezen, niet alleen indirect de gebruiker identificeert, maar ook (potentieel) de gebruiker lokaliseert. Het is immers vaak mogelijk eindapparatuur (en dus de persoon die er gebruik van maakt) te lokaliseren aan de hand van het IP-adres dat eraan is toegekend. De systematische verzameling van aan de bron van de verbinding toegewezen IP-adressen en de tijdsregistratie ervan maken het dus mogelijk de bewegingen van de gebruikers van deze diensten te volgen ; dit vormt een bijzonder belangrijke inmenging in het recht op privacy van deze gebruikers.

25. Dit betekent een radicale verandering ten opzichte van het paradigma van, en de privacyregels die zijn opgelegd door, de e-privacyrichtlijn[8]. **De Autoriteit benadrukt de noodzaak van een grondig**

overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd en met uitzondering van audiovisuele en auditieve mediadiensten, de volgende soorten diensten omvat:
a) internettoegangsdienst;
b) interpersoonlijke communicatiedienst; en
c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt ».

[7] De Autoriteit plaatst vraagtekens bij de mogelijk zeer ruime reikwijdte van deze definitie wanneer de telecomwet niet definieert wat wordt bedoeld met «*diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt* ».

[8] Zie in dit verband de opmerking van het HvJEU in het arrest van 6 oktober 2020 : « […] les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée […] » (§ 155).

parlementair debat over de gevolgen van deze wijziging, met name wat betreft het recht op privacy en het recht op vrijheid van meningsuiting[9]. In ieder geval herinnert de Autoriteit eraan dat inmenging in de rechten en vrijheden van de betrokken personen alleen toelaatbaar is indien zij noodzakelijk is en in verhouding staat tot de nagestreefde doelstelling van algemeen belang.

B. Aangaande amendement nr. 1

26. Amendement nr. 1 vervangt artikel 126 van de telecomwet. Deze bepaling **beoogt operatoren** die elektronische-communicatiediensten aan eindgebruikers aanbieden, alsmede operatoren die de elektronische-communicatienetwerken aanbieden die het aanbieden van dergelijke diensten mogelijk maken, **te verplichten inschrijvingsgegevens van abonnees en identificatiegegevens van eindgebruikers te bewaren**, alsmede **technische gegevens aan de hand waarvan de eindapparatuu**r van de eindgebruiker of de apparatuur die zich het dichtst bij die eindapparatuur bevindt, kan worden geïdentificeerd, **doch uitsluitend voor zover die operatoren dergelijke gegevens verwerken of genereren** in het kader van de levering van dergelijke diensten of netwerken (nieuw artikel 126, § 1).

27. Wat betreft het feit dat het nieuwe artikel 126, § 1, vereist dat bepaalde gegevens worden verzameld, maar alleen voor zover deze operatoren dergelijke gegevens verwerken of genereren in het kader van het aanbieden van deze diensten of netwerken, merkt de Autoriteit op dat operatoren gegevens kunnen genereren en verwerken (maar soms slechts gedurende enkele seconden) en ervoor kiezen om deze gegevens na deze verwerking niet te registreren om redenen van veiligheid, privacy of kosten. **De Autoriteit herinnert eraan dat het opleggen van de bewaring van dergelijke gegevens die de operatoren om de bovenvermelde redenen niet wensen te bewaren, een bijzonder belangrijke inmenging vormt in de persoonlijke levenssfeer van alle personen die gebruik maken van elektronische-communicatiediensten. Enerzijds is er geen garantie dat deze inmenging in het privéleven doeltreffend zal zijn om het nagestreefde doel te bereiken, aangezien er altijd mogelijkheden zullen zijn om communicatiemiddelen te vinden die aan het overheidstoezicht ontsnappen.** Anderzijds merkt de Autoriteit op dat **het bewaren van dergelijke gegevens een aanzienlijk risico inhoudt**, niet alleen wat de **persoonlijke levenssfee**r betreft, maar ook op het gebied van **informatiebeveiliging**, hetgeen **aanzienlijke**

[9] Hoewel de verplichting om gebruikers van een elektronische-communicatiedienst te identificeren niet rechtstreeks ingrijpt in het recht op vrije meningsuiting, merkt de Autoriteit op dat een dergelijke verplichting een "**chilling effect**"(d.w.z. een " afschrikkend effect" of een " remmend effect") zou kunnen hebben op de uitoefening van het recht op vrije meningsuiting via elektronische-communicatiemedia. Het bestaan van een dergelijk afschrikkend effect op de uitoefening van een grondrecht of een fundamentele vrijheid kan volgens de rechtspraak van het HvJEU of het EVRM worden gekwalificeerd als een inmenging in het recht of de vrijheid (in dit geval het recht op vrijheid van meningsuiting). Over de erkenning dat de vaststelling van maatregelen met een afschrikkende werking op de uitoefening van een grondrecht of fundamentele vrijheid een inmenging in de uitoefening van dat recht vormt, zie met name voor de rechtspraak van het HvJEU, 18 juni 2020, zaak. " Commissie v. Hongarije" en, voor jurisprudentie van het EHRM, (G.C.), 12 februari 2008, App. nr. 14277/04, Zaak «Guja vs. Moldavie ».

financiële gevolgen kan hebben voor de operatoren, die daarom extra beveiligingsmaatregelen moeten nemen. Deze extra kosten kunnen uiteindelijk door de consumenten worden gedragen als gevolg van hogere prijzen voor elektronische communicatiediensten. Deze extra kosten kunnen er ook toe leiden dat gratis en non-profit elektronische communicatiediensten[10], zoals Signal of Tor[11], hun diensten niet langer kunnen aanbieden aan gebruikers in België. **Om te voorkomen dat de rechten en vrijheden van de betrokkenen onevenredig worden aangetast** en om het risico van gegevensinbreuken tot een minimum te beperken, is de Autoriteit van mening dat operatoren voor de behoeften van de autoriteiten alleen verplicht zouden moeten worden tot het bewaren van abonneegegevens en gegevens waarmee eindgebruikers kunnen worden geïdentificeerd, alsmede technische gegevens waarmee de eindapparatuur van eindgebruikers of de apparatuur die zich het dichtst in de buurt van deze eindapparatuur bevindt, kan worden geïdentificeerd, **alleen voor zover zij deze gegevens voor hun eigen behoeften genereren en bewaren, en uiteraard op voorwaarde dat deze bewaring in overeenstemming is met de beginselen van noodzakelijkheid en evenredigheid**.

28. Terwijl het ontwerp van herstelwet voorzag in een delegatie aan de Koning om te bepalen welke gegevens door de operatoren moeten worden bewaard ter uitvoering van artikel 126 van de telecomwet, voorziet de wijziging in de opsomming, in de telecomwet zelf, van de categorieën van gegevens die door de operatoren moeten worden bewaard ter uitvoering van deze bepaling, teneinde te voldoen aan de vereisten van het legaliteitsbeginsel, zoals geïnterpreteerd door het Grondwettelijk Hof in zijn arrest nr. 158/2021. Zoals de Regering uitlegt in haar verantwoording van het amendement zijn «*Om rekening te houden met dat arrest zijn de gegevens die zich voordien bevonden in de paragrafen 1 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, verplaatst geweest naar dat artikel 126*». Zo zijn **de meeste gegevens uit het amendement rechtstreeks overgenomen uit de artikelen 3 tot en met 6 van het besluit van 19 september 2013**, zoals dat had moeten worden gewijzigd bij het ontwerp van koninklijk besluit dat voor advies aan de Autoriteit was voorgelegd en waarover zij advies had uitgebracht in haar advies nr. 108/2021. Voor deze gegevens **verwijst de Autoriteit derhalve naar de overwegingen 92 tot en met 102 van haar advies nr. 108/2021 voor een onderzoek van het beginsel van de minimale gegevensverwerking** [12]**.**

---

[10] Deze diensten brengen hun gebruikers geen kosten in rekening en genereren geen winst uit reclame.

[11] De Autoriteit merkt bovendien op dat als deze diensten (waarvan zeker gebruik wordt gemaakt door mensen die strafbare feiten plegen, maar ook door journalisten, klokkenluiders, politieke activisten, mensen die opkomen voor rechten en vrijheden...) verplicht zouden zijn de IP-adressen te bewaren die verbinding maken met hun diensten, dit niet alleen hun exploitatiekosten aanzienlijk zou verhogen, maar zou dit ook een aanzienlijk risico inhouden voor de privacy in het geval van bijvoorbeeld een aanval door een buitenlandse inlichtingendienst (zonder dat de Belgische autoriteiten het nut van een dergelijke gegevensbewaring hebben aangetoond).

[12] De Autoriteit zou echter graag de dialoog voortzetten die de auteur van het amendement is begonnen over gegevens waarmee eindapparatuur van eindgebruikers technisch kan worden geïdentificeerd (d.w.z. gegevens zoals IMEI-, PEI- of MAC-adressen). In de motivering van het amendement verklaart de auteur van het amendement immers dat hij de redenering van de Autoriteit met betrekking tot deze gegevens niet kan volgen. De auteur van het amendement schrijft: «contrairement à ce que cette

29. Naast de gegevens die reeds in het koninklijk besluit van 19 september 2013 zijn opgesomd, **voorziet dit amendement in de verplichting om een aantal bijkomende gegevens te bewaren** (maar nog steeds slechts voor zover de operator deze gegevens verwerkt of genereert in het kader van de levering van de dienst), namelijk :

- **de eventuele alias die door de eindgebruiker is gekozen wanneer hij zich op de dienst abonneert of de dienst activeert, d.w.z. de naam waaronder de eindgebruiker zich bij andere eindgebruikers kenbaar maakt). In de verantwoording van het amendement, vermeldt de auteur «*Indien de eindgebruiker de mogelijkheid heeft om bij de activering van de dienst zijn alias te wijzigen, zal de operator zowel de alias bij de inschrijving als die bij de activering moeten bewaren* » ;**

- **het e-mailadres van de abonnee (als een contactgegeven van deze abonnee);**

- **het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden**.

30. De auteur van het amendement motiveert de noodzaak om deze gegevens te bewaren als volgt : «*Het frequente gebruik van valse identiteitsgegevens maakt het noodzakelijk de bewaarde identificatiegegevens te kunnen toetsen aan andere bij de operatoren beschikbare gegevens», waaronder de aliassen en het e-mailadres van de abonne*e. *Nog volgens de auteur van het amendement «Die bijkomende gegevens kunnen uitsluiten dat slachtoffers van identiteitsfraude onterecht worden betrokken als dader in een gerechtelijk dossier dat geen betrekking heeft op hen*. *De bijkomende gegevens voorkomen zo ook dat de privacy van deze onschuldige personen verder*

Autorité indique dans son avis, une telle donnée [ndlr : les numéros d'identification des terminaux des utilisateurs finaux] à elle seule ne permet pas de 'tracer' un terminal à travers l'ensemble des services de communications électroniques qu'il utilise. ***L'Autorité n'a jamais affirmé que ces données permettaient, <u>à elles seules,</u> de tracer un terminal à travers l'ensemble des services de communications utilisées***. In haar advies 108/2021 merkte de Autoriteit in overweging 102 het volgende op: «*De identificatienummers van de eindapparaten van de eindgebruikers zijn een unieke identificatie van de eindapparaten waarmee een apparaat kan worden 'getraceerd' via alle elektronische communicatiediensten die het gebruikt* en het is omwille van deze vaststelling dat de Autoriteit van mening is dat voor de verplichting om dergelijke technische gegevens ter identificatie van de eindgebruikersapparatuur te bewaren, dezelfde regels moeten gelden als die welke het HvJEU heeft vastgesteld voor het bewaren van IP-adressen die aan de bron van een verbinding worden toegewezen. De identificatienummers van de eindgebruikersterminals maken, in combinatie met andere gegevens, de tracering van deze terminals door alle gebruikte communicatiediensten mogelijk. De situatie is vergelijkbaar voor IP-adressen die zijn toegewezen aan de bron van de verbinding: met deze gegevens <u>alleen</u> kan het surftraject van een gebruiker, en bijgevolg zijn onlineactiviteit, niet uitputtend worden getraceerd. Maar in combinatie met andere gegevens kunnen de IP-adressen die aan de bron van een verbinding zijn toegewezen, het traject van een internetgebruiker op het internet onthullen. De parallel die de Autoriteit in haar Advies nr. 108/2021 trekt tussen de identificatienummers van eindapparatuur en de IP-adressen die aan de bron van de verbinding zijn toegewezen, lijkt derhalve relevant. Tijdens een informatie-uitwisseling met de afgevaardigde van de minister in het kader van de voorbereiding van de zaak die tot advies nr. 108/2021 heeft geleid, heeft deze overigens erkend dat de redenering van het HvJEU met betrekking tot IP-adressen kan worden gevolgd met betrekking tot de andere technische gegevens die nodig zijn om de eindgebruiker, de eindapparatuur en de gebruikte elektronische-communicatiedienst te identificeren. **Hieruit volgt, zoals de Autoriteit reeds in haar advies nr. 108/2021 heeft aangegeven, dat de bewaring van dergelijke gegevens alleen mag worden opgelegd om een doelstelling van bijzonder belang na te streven (zoals de bestrijding van zware criminaliteit), dat de duur van de bewaring strikt moet worden beperkt in het licht van die doelstelling en dat moet worden voorzien in strikte voorwaarden en waarborgen voor het gebruik van dergelijke gegevens** (zie HvJEU, arrest van 6 oktober 2020, § 156)**.**

zou worden geschonden door meer indringende, navolgendeonderzoeksmaatregelen zoals een interceptie van hun communicatie of een huiszoeking. ***De Autoriteit neemt hiervan kennis.***.

31. In het **nieuwe artikel 126, §2** van de telecomwet, dat bij amendement 1 is ingevoegd, **worden de bewaartermijnen van de gegevens vastgesteld**. **Voor alle gegevens**, met uitzondering van IP-adressen die zijn toegewezen aan de bron van een verbinding en unieke identificatoren van de eindapparatuur van de gebruiker, **bedraagt de bewaarperiode 12 maanden na het einde van de dienst**. Voor **IP-adressen toegewezen aan de bron van een verbinding** en de **unieke identifiers van de eindapparatuur van de gebruiker (**d.w.z. : International Mobile Equipment Identity ("IMEI"), Permanent Equipment Identifier ("PEI"), Network Access Controlleradress ("MAC"), is bewaartermijn is **12 maanden na het einde van de sessie**. Voor **MAC-adressen** bedraagt de bewaartermijn **6 maanden na het einde van de sessie**, indien de exploitant nog andere identificatiegegevens van de eindapparatuur van de gebruiker bewaart[13]. **De Autoriteit neemt akte van deze bewaartermijnen**.

C. Aangaande de amendementen 2 en 3

32. Amendement 2 is bedoeld ter vervanging van §2 van artikel 126/1 van de telecomwet, zoals gewijzigd bij de herstelwet. Ter herinnering: het nieuwe artikel 126/1 van de telecomwet, zoals gewijzigd bij de herstelwet, **verplicht** operatoren om in principe **gedurende 12 maanden** de **verkeers- en locatiegegevens** te bewaren van **alle communicatie vanuit of naar** een van de in het artikel opgesomde **geografische gebieden[14].** Dergelijke gegevens mogen alleen worden bewaard indien de operatoren ze reeds genereren of verwerken in het kader van de levering van de elektronische-communicatiediensten die zij aanbieden of de elektronische-communicatienetwerken die zij ter beschikking stellen[15]. Deze bewaring is verplicht «*ter de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid en de vrijwaring van vitale belangen van een natuurlijk persoon*». Het nieuwe artikel 126/1 van de telecomwet is dus bedoeld om **een geografisch gerichte preventieve bewaring van verkeers- en locatiegegevens op te leggen** met het oog op bijzonder belangrijke doelstellingen, zoals de bestrijding van zware criminaliteit. De Autoriteit verwijst naar de **overwegingen 106 tot en**

---

[13] Wat het bewaren van MAC-adressen betreft, merkt de Autoriteit op dat MAC-adressen zeer regelmatig worden gewijzigd (sinds 2014). Het verzamelen van deze informatie vereist dan ook massale gegevensopslag en is van weinig nut. zie bijvoorbeeld, https://en.wikipedia.org/wiki/MAC_address#Randomization: "MAC address randomization during scanning was added in Android starting from version 6.0,[19] Windows 10,[21] and Linux kernel 3.18.[22].

[14] Tenzij een andere duur zou worden voorzien in dit nieuwe artikel 126/1 van de telecomwet. Deze bepaling voorziet in bepaalde omstandigheden in kortere bewaartermijnen. Zie het nieuwe artikel 126/1 §3, 1° van de telecomwet.

[15] In de memorie van toelichting wordt het volgende uitgelegd: «*de gegevens worden door de betrokken operatoren slechts bewaard voor zover zij door hen werden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, en alleen in de vooraf afgebakende geografische gebieden. Met andere woorden, er is geen verplichting om de gegevens te bewaren wanneer zij:*

1° niet worden gegenereerd of verwerkt door de betrokken operatoren,

2° niet worden gegenereerd of verwerkt in de in paragraaf 3 bepaalde geografische gebieden

met 130 van haar advies nr. 108/2021, waarin zij onderzocht of deze bepaling voldoet aan de vereisten die voortvloeien uit het recht op gegevensbescherming, zoals dat met name is vastgelegd in het Handvest van de grondrechten van de Europese Unie en de e-privacyrichtlijn. **De Autoriteit merkt op dat zij onder meer fundamentele bezwaren tegen deze bepaling had**, met name dat de criteria die in de ontwerp-herstelwetgeving worden gebruikt om te bepalen in welke geografische gebieden een preventieve verplichting om verkeersgegevens te bewaren wordt opgelegd, de facto zouden kunnen leiden tot de herinvoering van een quasi gegeneraliseerde en ongedifferentieerde verplichting om verkeersgegevens te bewaren. Bovendien wijst de Autoriteit erop dat sommige operatoren van elektronische-communicatiediensten, zoals Signal, geen toegang hebben tot de locatiegegevens van hun abonnees. Op grond van het nieuwe artikel 126/1 van de telecomwet zouden deze diensten dus preventief de verkeersgegevens van al hun abonnees moeten verzamelen ; dit zou indruisen tegen het evenredigheidsbeginsel, zoals geïnterpreteerd door het HJEU[16].

33. In het herstelwetsontwerp was erin voorzien dat aan de Koning de bevoegdheid zou worden gedelegeerd om te bepalen welke gegevens ter uitvoering van deze bepaling moesten worden bewaard. **De regering heeft naar aanleiding van arrest nr. 158/2021 besloten in de wet zelf een opsomming te geven van de metagegevens die ter uitvoering van deze bepaling moeten worden bewaard**. Zo bepaalt artikel 126/1, lid 2, zoals vervangen bij amendement 2, dat « *De elektronische-communicatiemetagegevens, met inbegrip van de metagegevens voor de oproeppogingen zonder resultaat, waarop de in paragraaf 1 bedoelde bewaarplicht van toepassing is,worden opgesomd in artikel 126/2*». Amendement 3, dat ertoe strekt artikel 126/2 in de telecomwet op te nemen, bevat een lijst van de gegevens die overeenkomstig artikel 126/1 moeten worden bewaard. Zoals het geval is voor de gegevens die overeenkomstig artikel 126 moeten worden bewaard, **zijn de meeste van de in amendement 3 vermelde gegevens rechtstreeks overgenomen uit de artikelen 3 tot en met 6 van het besluit van 19 september 2013**, zoals het had moeten worden gewijzigd bij het ontwerp van koninklijk besluit dat voor advies aan de Autoriteit is voorgelegd en waarover zij advies nr. 108/2021 uitbracht. Voor de analyse van deze gegevens verwijst de Autoriteit derhalve naar haar advies nr. 108/2021[17].

34. **Er zijn evenwel meerdere nieuwigheden:**

[16] Zie met name HvJEU, arrest van 6 oktober 2020, § 141 e.v. De Autoriteit verwijst bovendien naar de overwegingen 129 en 130 van haar advies 108/2021, waarin zij opmerkt dat de bepaling «*Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden» ontoelaatbaar is.*

[17] Zij merkt tevens op dat de auteur van het amendement rekening heeft gehouden met haar opmerking dat «*de bewaring van verkeersgegevens geen specifieke url van de door de betrokkenen bezochte webpagina's mag bevatten of het mogelijk maken die url's af te leiden*». Het amendement nr. 3 vermeldt inderdaad «*voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen*» (onderstreept door de Autoriteit). Voor internettoegangsdiensten mag het IP-adres van de ontvanger (dat de URL van de bezochte webpagina zou identificeren) niet worden opgeslagen.

- De bewaring van «d*e eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst*» (2°)

- de unieke identifier voor de individuele oproepen ("SIP call ID") (4°)[18]

- de gegevens voor het identificeren en het lokaliseren van de cellen of andere netwerkaansluitpunten, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties (terwijl in de vorige versie alleen de locatie van cellen of andere netwerkaansluitpunten die aan het begin en het einde van het gesprek worden gebruikt, moest worden bijgehouden)[19] (7°)

- voor wat betreft de mobiele elektronische- communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens van het opstarten van die apparatuur, en het moment waarop de verbinding van deze eindapparatuur met het netwerk wordt verbroken wegens het uitschakelen van die apparatuur (9°)[20]

- voor wat betreft de mobiele elektronische-communicatiediensten, de locatie van de eindapparatuur en de datum en het tijdstip van deze locatie telkens wanneer de operator wil weten welke eindapparatuur is verbonden met zijn netwerk (10°)[21]

- de bewaring van elk gegeven met een gelijkwaardige functie [maar waavoor?], wanneer een van de voormelde gegevens niet beschikbaar is (11°)

---

[18] Het bewaren van deze gegevens wordt als volg verantwoord: «*De "SIP call ID" maakt het mogelijk elke individuele Voice-over-IP-oproep op een betrouwbare manier te identificeren. De "SIP call ID" is een belangrijk te bewaren gegeven aangezien in de toekomst het grootste deel van de telefonische oproepen SIP-verkeer zal worden.*».

[19] De verantwoording van het amendement zegt daarover het volgende: «*Een nieuwe vereiste wordt toegevoegd ten opzichte van het koninklijk besluit van 2013: de operatoren moeten voortaan de locatie van de cellen en andere netwerkaansluitpunten bewaren gedurende de communicatie (bijvoorbeeld de tussenliggende masten, of de wifirouters in het kader van nomadische diensten) en niet uitsluitend hun locatie bij aanvang en einde van de communicatie. Het nut van een dergelijke vereiste wordt volledig duidelijk wanneer de eindgebruiker zich verplaatst. Dergelijke informatie is van cruciaal belang voor de veiligheidsdiensten. De locatiegegevens die de operatoren moeten bewaren buiten elke communicatie worden bepaald in paragraaf 2, 10°. Artikel 5, § 2, 3°, van het KB van 2013 vermeldde de identificatie en de lokalisering van het netwerkaansluitpunt gebruikt door de eindgebruiker enkel bij de aanvang en op het einde van de verbinding. In het kader van de 2G- en 3G-technologie maakte dit inderdaad mogelijk om de met deze technologie uitgevoerde communicatie te lokaliseren. Dit type van gebruik is voorbijgestreefd sinds het wijdverspreide gebruik van smartphones met permanente dataverbinding, omdat met deze technologie een datasessie vele uren kan duren (soms meer dan 12 uur).*

[20] De verantwoording van het amendement zegt daarover het volgende: «*Terwijl de artikelen 4, § 2, 6° en 5, § 2, 3° van het koninklijk besluit van 2013 een brede verplichting omhelsden voor de operatoren inzake bewaring van verbindingsgegevens, schrijft de nieuwe paragraaf 2, 9° van het ontworpen artikel 126/2 de bewaring voor van bepaalde verbindingsgegevens los van een communicatie, namelijk de verbindings- /afschakelgegevens die worden gegenereerd bij het aan- of uitzetten van de mobiele telefoon.* ». *Het gevolg daarvan is dat een gebruiker verkeerdelijk gelokaliseerd zou kunnen worden op een plek, terwijl hij zich daar al ettelijke uren niet meer bevindt. Deze foutieve plaatsbepaling riskeert gevolgen à charge of à décharge voor de burgers met zich te brengen.*

[21] De verantwoording van het amendement zegt daarover het volgende: «*Zo bepaalt de nieuwe paragraaf 2, 10°, van het ontworpen artikel 126/2 de bewaring van de locatie van de eindapparatuur buiten elke communicatie in het kader van de handelingen die de operator regelmatig uitvoert om te weten welke eindapparatuur zich op zijn netwerk bevindt. Dat is technisch noodzakelijk om de goede werking ervan te behouden, om een hoog niveau van dienstverlening te behouden, om de oproepen en communicatie die ze moeten behandelen, snel te verwerken, enz. Daartoe worden verscheidene methodes gebruikt. Het kan bijvoorbeeld gaan om "LBS" ("Localisation Base Services") of "paging". De frequentie en de methode van deze handelingen verschillen. Ze hangen af van de technische vereisten die inherent zijn aan het netwerk van de operator, zoals het type technologie dat wordt gehanteerd (2G, 3G, 4G, enz.) of de dichtheid van de gebruikers op een deel van het netwerk.* ».

35. Ten eerste merkt de Autoriteit op dat uit de **motivering bij het amendement niet blijkt waarom deze noodzakelijk is om het doel van de bewaring van deze gegevens te bereiken,** namelijk de bestrijding van zware criminaliteit, de **datum en het uur te bewaren van de aansluiting** van de eindapparatuur op het net ten gevolge van het opstarten van die apparatuur en **het uur van de ontkoppeling van die apparatuur** van het net ten gevolge van het uitschakelen van die apparatuur (9°), alsook de locatie van de eindapparatuur en de datum en het uur van die locatie telkens wanneer de operator de aanwezigheid van de eindapparatuur op zijn net tracht na te gaan (10°). **Ofwel kan de auteur van het amendement aantonen hoe de bewaring van deze categorieën gegevens noodzakelijk is en in verhouding staat tot het nagestreefde doel, en wordt deze uitleg toegevoegd in de motivering van de wijziging, ofwel moet de toevoeging van deze nieuwe categorieën gegevens (of ten minste van die waarvoor de auteur de bewaring niet kan rechtvaardigen) worden geschrapt**.

36. Verder merkt de Autoriteit op over de opgesomde gegevens onder 11° van artikel 126/2 § 2 (*wanneer een van de voormelde gegevens niet beschikbaar is, elk gegeven met een gelijkwaardige functie*) dat de definitie ervan **niet voldoende voorspelbaar** is om de betrokkenen in staat te stellen te bepalen welke gegevens de operatoren daadwerkelijk op deze basis zullen bewaren. Gezien de bijzonder grote inmenging die wordt veroorzaakt door de bewaring van verkeers- en locatiegegevens op grond van artikel 126/1 (aan de hand waarvan kan worden nagegaan wie met wie heeft gecommuniceerd, hoe lang, en van waar), is het echter van essentieel belang dat de regelgeving betreffende deze gegevensverwerking bijzonder nauwkeurig en voorspelbaar is. **Het amendement zal worden gewijzigd om artikel 126/2, § 2, 11° te schrappen[22].**

D. Aangaande amendement nr. 6

37. Amendement nr. 6 vervangt artikel 127 van de Telecomwet en beoogt tegemoet te komen aan de vernietiging door het Grondwettelijk Hof van artikel 2 van de wet van 1 september 2016 « *tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst* » zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen.

38. Artikel 127 van de telecomwet wil **de operatoren verplichten hun abonnees** te identificeren ten behoeve van de autoriteiten of informatie te bewaren die de autoriteiten in staat stellen hen later te

[22] Indien de auteur de aanbeveling van de Autoriteit om artikel 126/2, § 2, 11° te schrappen niet volgt, dient het dispositief ten minste als volgt te worden aangevuld : Met het oog op de naleving van het beginsel van de minimale gegevensverwerking wordt aanbevolen dat «*wanneer geen van de bovengenoemde gegevens beschikbaar is, gegevens met een gelijkwaardige functie mogen worden gebruikt, op voorwaarde dat deze niet meer informatie bevatten dan de bovengenoemde gegevens*».

identificeren[23]. In tegenstelling tot de vorige versie van deze bepaling (in het ontwerp van herstelwet) geeft de versie van artikel 127, die in amendement nr. 6 is opgenomen, **een opsomming van de identificatiegegevens** die door de operatoren moeten worden verwerkt en bewaard in het kader van de verplichting om abonnees en eindgebruikers van hun diensten te identificeren.

39. De verantwoording bij het amendement zegt hierover het volgende «*Paragraaf 1 van artikel 127 is een algemene paragraaf en beschrijft het toepassingsgebied ervan (onder andere de operatoren en elektronische-communicatiediensten waarop het van toepassing is). De paragrafen 2 tot 9 hebben betrekking op de identificatie door een operator van de abonnee (de persoon die het contract met de operator sluit). Paragraaf 10 is gewijd aan de identificatie van de effectieve gebruiker van de dienst. Paragraaf 11 is een algemene paragraaf en beschrijft de toepasselijke sancties wanneer de operatoren of de abonnees hun verplichtingen niet nakomen*».

1. betreffende de uitbreiding van de verplichting tot identificatie van abonnees en eindgebruikers van elektronische-communicatiediensten

40. De Autoriteit merkt op dat **het nieuwe artikel 127 de verplichting om abonnees en eindgebruikers van elektronische-communicatiediensten te identificeren aanzienlijk uitbreidt** :
    - Ten eerste zal, na de wijziging van de definities van "*operator*" en "*elektronische-communicatiedienst*" (zie overwegingen 23-24 hierboven), **de opgelegde identificatieplicht in het nieuwe artikel 127 betrekking hebben op de gebruiker van veel meer elektronische-communicatiediensten dan in het huidige regelgevingskader is bepaald.** Deze verplichting zal namelijk gelden voor alle elektronische-communicatiediensten die beantwoorden aan de nieuwe definitie van dit begrip, waaronder met name interpersoonlijke communicatiediensten die niet op nummers zijn gebaseerd (de " OTT ", zoals WhatsApp, Messenger, Signal, Telegram, Tik Tok, ...) en communicatiediensten die worden aangeboden om " M2M "-toepassingen (internet van dingen/connected objects) mogelijk te maken. Voorts dient te worden benadrukt dat de identificatieplicht zal gelden voor zowel elektronische

[23] *De autoriteiten die bevoegd zijn om de identiteit van abonnees en eindgebruikers van elektronische-communicatiediensten te ontvangen, zijn de volgende :*
« *1° de inlichtingen- en veiligheidsdiensten, met het oog op de uitvoering van de opdrachten die hen zijn toevertrouwd door de organieke wet van 30 november 1998 betreffende de inlichtingen- en veiligheidsdiensten;*
2° de bevoegde autoriteiten voor de preventie van ernstige bedreigingen van de openbare veiligheid;
3° de autoriteiten belast met de vrijwaring van de vitale belangen van natuurlijke personen;
4° de instanties die belast zijn met het onderzoek naar een storing in de veiligheid van het netwerk of de dienst;
5° de administratieve of gerechtelijke autoriteiten die belast zijn met het voorkomen, onderzoeken, opsporen of vervolgen van een strafbaar feit dat online of via een elektronisch communicatienetwerk of een elektronische communicatiedienst is gepleegd;
6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een daad die een ernstig misdrijf vormt;
7° de administratieve overheden die belast zijn met de vrijwaring van een belangrijk economisch of financieel belang van de Europese Unie of België, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid ;
8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van een strafbaar feit dat geen ernstig misdrijf is (artikel 127/1, eerste lid).

communicatiediensten die tegen betaling als deze die kosteloos worden geleverd. Ter vergelijking, de huidige versie van artikel 127 van de telecomwet[24] delegeert aan de Koning de taak om de technische en administratieve maatregelen te bepalen die aan de operatoren worden opgelegd om de identificatie van de eindgebruiker mogelijk te maken. Deze bepaling is bij het koninklijk besluit van 27 november 2016[25] alleen ten uitvoer gelegd voor elektronische-communicatiediensten die worden aangeboden op basis van een voorafbetaalde kaart voor mobiele telefonie. Bovendien geldt in de huidige normatieve context voor houders van een SIM-kaart die uitsluitend voor "M2M communicatie" wordt gebruikt, geen identificatieplicht[26].

- Ten tweede **zullen meer autoriteiten toegang kunnen krijgen tot de identificatiegegevens** van abonnees van elektronische-communicatiediensten dan op grond van de huidige versie van de artikelen 126 en 127 het geval is.

- Ten derde zegt de auteur van het amendement nr. 6 «*Het oude artikel 127, § 2, bevatte een verbod voor de operatoren om de identificatie van de eindgebruikers te bemoeilijken of onmogelijk te maken*. Het ***nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte identificatiemethode)*** ».

- Ten vierde verbiedt het nieuwe artikel 127 § 1, op straffe van strafrechtelijke sancties, de distributie in België van voorafbetaalde kaarten of abonnementen waarmee eindgebruikers een elektronische-communicatiedienst kunnen gebruiken, of van daarmee verbonden voorwerpen die het gebruik van een internettoegangsdienst of een interpersoonlijke-communicatiedienst mogelijk maken, zonder de toestemming te hebben verkregen van de onderneming die deze openbare elektronische-communicatiedienst aanbiedt. De onderneming die haar toestemming geeft, moet worden beschouwd als een operator die gebonden is door opgelegde verplichting krachtens dit nieuwe artikel 127. **Dit verbod is bedoeld om te voorkomen dat de verplichting van de operatoren om de eindgebruikers van de door hen aangeboden elektronische-communicatiediensten, te identificeren, wordt omzeild**.

41. Deze uitbreiding van de verplichting tot identificatie van de eindgebruikers van elektronische-communicatiediensten leidt tot een **aanzienlijke toename van de inmenging in hun rechten en**

[24] Dat wil zeggen deze die door het Grondwettelijk Hof in zijn arrest nr. 158/2021 nietig is verklaard, maar alleen voor zover deze bepaling niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking worden genomen.
[25] KB van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart (hierna het koninklijk besluit 27 november 2016).
[26] Artikel 1, derde lid van het koninklijk besluit van 27 september 2016.

vrijheden[27]. De doelstellingen die met deze uitbreiding - en meer in het algemeen met de identificatie van gebruikers van elektronische-communicatiediensten - worden nagestreefd, zijn zeker legitiem. Maar de rechtmatigheid van de nagestreefde doelstellingen volstaat niet om inmenging in de rechten en vrijheden van de betrokken personen te rechtvaardigen. Daarnaast moet erop worden toegezien dat de inmenging passend/relevant, noodzakelijk en, ten slotte, strikt evenredig aan het nagestreefde doel is. Met andere woorden, **het doel op zich heiligt de middelen niet**. De Autoriteit verzoekt de parlementsleden derhalve **een grondige analyse te maken van de relevantie, noodzaak en evenredigheid van een dergelijke uitbreiding van de verplichting om de eindgebruikers van elektronische-communicatiediensten te identificeren, en daarbij met name rekening te houden met de gevolgen van deze uitbreiding voor de uitoefening van het recht op privacy en het recht op vrijheid van meningsuiting**. In deze analyse verzoekt de Autoriteit de parlementsleden ook rekening te houden met het feit dat criminelen die de controle van elektronische communicatiemiddelen door de autoriteiten willen vermijden, andere communicatiemiddelen zullen vinden waarmee zij anoniem kunnen blijven. De **Autoriteit verzoekt de parlementsleden dan ook bijzonder voorzichtig te zijn en de vrijheden van bijna de gehele bevolking niet te beknotten door een maatregel goed te keuren** (verplichting tot identificatie van de gebruikers van alle elektronische communicatie) **als blijkt dat deze maatregel in feite niet relevant en noodzakelijk is, met name omdat "criminelen" redelijkerwijs andere communicatiemiddelen zouden kunnen vinden om te ontsnappen aan de "bewaking" van de elektronische-communicatiediensten door de autoriteiten**.

2. Over de kwaliteit van de identificatie van abonnees

42. De Autoriteit acht het tevens van essentieel belang de aandacht van de parlementsleden te vestigen op het feit dat **de identificatie van de abonnee van een elektronische-communicatiedienst niet noodzakelijkerwijs de daadwerkelijke gebruiker van die dienst identificeer**t. Het nieuwe artikel 127 § 10 van de telecomwet beoogt zeker een vermoeden te creëren volgens hetwelk «*Behoudens tegenbewijs (...) de geïdentificeerde persoon geacht (wordt) zelf de elektronische-communicatiedienst te gebruiken* » (zie infra, overw. 78). In de praktijk is het echter niet ongewoon dat de gebruiker van een elektronische-communicatiedienst niet dezelfde is als de persoon die zich op de dienst heeft geabonneerd. Er bestaat derhalve een **reëel risico** dat de eindgebruiker **niet met zekerheid kan worden geïdentificeerd** en dat de kwaliteit van de identificatiegegevens van de eindgebruiker **in twijfel kan worden getrokken**. De onzekere kwaliteit van de identificatiegegevens **zal groter zijn** naarmate de abonnee meer wordt geïdentificeerd door middel van een indirecte identificatiemethode. Het identificeren van de persoon "achter" een IP-adres, een telefoonnummer of

[27] De Autoriteit herinnert er in dit verband aan dat het HvJEU in zijn Quadrature du Net-arrest heeft opgemerkt dat «internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop (moeten) kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld» (§ 155).

de referentie van een banktransactie maakt het immers niet mogelijk om met zekerheid de persoon te identificeren die daadwerkelijk van de elektronische-communicatiedienst gebruik heeft gemaakt. **In deze omstandigheden, waarin de kwaliteit van de identificatie van de werkelijke gebruiker** van de elektronische-communicatiedienst **onzeker lijkt**, dringt de Autoriteit erop aan dat de parlementsleden nadenken over, en verantwoording afleggen van, **de noodzaak van de inmenging i**n het recht op bescherming van persoonsgegevens van abonnees van elektronische-communicatiediensten.

43. Amendement nr. 6 maakt een **onderscheid tussen de modaliteiten** van de verplichting tot identificatie van de abonnee **naargelang** de elektronische-communicatiedienst **gratis dan wel tegen betaling is**[28]. In het geval van een **betalende dienst** vereist het nieuwe artikel 127 van de telecomwet in principe dat de operatoren hun abonnees identificeren aan de hand van een **directe of indirecte identificatiemethode**[29] «*of door de vergaring en bewaring van het kenmerk van de betalingsverrichting, de naam, de voornaam, de geboorteplaats en -datum van de abonnee*» (die een indirecte identificatiemethode is) (op grond van het feit dat volgens het beginsel van de minimale gegevensverwerking, «*de geboorteplaats- en datum*»,niet bewaard moegen worden, zie overw. 75). Het nieuwe artikel 127 bepaalt evenwel dat voor bepaalde elektronische-communicatiediensten waarvoor moet worden betaald, de identificatie op andere, in het artikel genoemde manieren kan geschieden. Wanneer de elektronische-communicatiedienst **gratis** is, identificeert de operator zijn abonnees aan de hand van een van de **indirecte identificatiemethode**[30] als bedoeld in § 9 van dit artikel[31] met inbegrip van het bewaren van het IP-adres dat is gebruikt voor het aanmaken van het

[28] Het nieuwe artikel 127 geeft aan elektronische communicatiedienst deze definitie: «*een elektronische-communicatiedienst waarbij de abonnee moet betalen aan de operator om de dienst te gebruiken of te blijven gebruiken, evenals elke elektronische-communicatiedienst die samen met deze dienst zonder meerkosten door de operator wordt aangeboden aan de abonnee.*

[29] In het nieuwe artikel 127 wordt de methode van directe identificatie als volgt gedefinieerd: «*methode waarbij de operator betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon die zijn abonnee is of die optreedt voor rekening van zijn abonnee die een rechtspersoon is om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval, een kopie van het identificatiedocument van deze natuurlijke persoon».*

[30] In het nieuwe artikel 127 wordt de methode van indirecte identificatie als volgt gedefinieerd: «*indirecte identificatiemethode: methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen*».

[31] De keuze van de wetgever om identificatie via een indirecte methode op te leggen, in plaats van via een methode van directe identificatie, houdt verband met het inachtnemen van de persoonlijke levenssfeer van de gebruiker. Uit de verantwoording van het amendement bljkt immers «*De operatoren die gratis diensten aanbieden zijn over het algemeen operatoren die interpersoonlijke communicatiediensten aanbieden die nummeronafhankelijk zijn (de "OTT's"). Zij beschikken doorgaans niet over de gegevens van burgerlijke identiteit van hun abonnees (of toch niet over gegevens waarvan de betrouwbaarheid geverifieerd is) noch over een kopie van hun identificatiedocumenten, aangezien dat niet noodzakelijk is om hun diensten te kunnen aanbieden. De omzet die zulke operatoren boeken, komt over het algemeen van de verwerking van de gegevens van de abonnee en het verzenden van reclame naar die laatste. De regering wenst te vermijden dat de operatoren van wie het commerciële model gebaseerd is op de verwerking van de abonneegegevens, een directe identificatiemethode instellen, aangezien dat zou betekenen dat ze de (soms talrijke) gegevens die ze al over de abonnee in handen hebben, zouden kunnen in verband brengen met de identiteit van die abonnee, waardoor de verwerking van zijn gegevens gevoeliger zou worden. De indirecte identificatie is het meer geschikt voor de gratis diensten, aangezien deze identificatiemethode als voordeel heeft dat de operator zelf de identiteit van zijn abonnee niet kent wanneer het niet nodig is dat hij die kent*» (het is de Autoriteit die onderlijnt). De Autoriteit neemt nota van de bereidheid van de auteur van het amendement om de doelstelling van de identificatie van abonnees ten behoeve van de autoriteiten te combineren met het beginsel van de minimale gegevsverwerking. Zij wijst er echter op dat sommige operatoren een elektronische-communicatiedienst, zoals Signal of Tor, aanbieden zonder gegevens van hun abonnees te verzamelen en dat zij geen winstoogmerk hebben (zij verdienen geen geld met het zenden van advertenties aan hun abonnees).

account dat het gebruik van de elektronische-communicatiedienst mogelijk maakt en de IP-adressen bij de bron van de verbinding, de tijdsaanduiding en, bij gedeeld gebruik van een IP-adres van een eindgebruiker, de poorten die daaraan zijn toegewezen of het verzamelen en bewaren van het telefoonnummer van de abonnee dat is toegewezen in het kader van een betaalde elektronische-communicatiedienst waarvoor een exploitant de abonnee moet identificeren (zie hieronder, overw. 72 en volgende in verband met deze opmerkingen).

3. *Over het (niet) bewaren van identificatiegegevens en -documenten door verkooppunten* (artikel 127, § 3, leden 1 en 2)

44. Het nieuwe artikel 127 §3, 1ste en 2de lid, bepaalt «*Het verkooppunt van elektronische-communicatiediensten bewaart noch identificatiegegevens noch kopieën van identiteitsstukken, die worden overgezonden naar de operator of naar de onderneming die een identificatiedienst verstrekt. Indien een rechtstreekse invoer in de computersystemen van de operator of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkooppunt van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd* ».

45. De Autoriteit **neemt nota van de verzekering** dat het verkooppunt van elektronische-communicatiediensten geen identificatiegegevens of kopieën van identiteitsdocumenten bewaart**.**

46. De Autoriteit herinnert er echter aan dat het **kopiëren van identiteitsdocumenten aanzienlijke risico's voor de rechten en vrijheden van de betrokken personen met zich meebrengt** (met name het risico van identiteitsfraude). Het maken van kopieën van identiteitsdocumenten moet daarom worden beperkt tot gevallen waarin dat strikt noodzakelijk is. In dit geval benadrukt de Autoriteit dat het de voorkeur zou verdienen te voorzien in een verplichting voor de verkooppunten om de identificatiegegevens rechtstreeks in te voeren in de door de operatoren overeenkomstig artikel 127[32] bij te houden gegevensbanken. **Het nieuwe artikel 127, §3, 1ste en 2de lid zal worden gewijzigd om de verkooppunten van elektronische-communicatiediensten te verplichten de identificatiegegevens van de abonnees rechtstreeks in te voeren in de**

[32] Indien het niet mogelijk is de verkooppunten een dergelijke verplichting op te leggen (die overeenkomstig de beginselen van noodzakelijkheid en evenredigheid zal moeten worden gerechtvaardigd aan de hand van feitelijke en concrete elementen), moet het maken van kopieën van identiteitsdocumenten op zijn minst met waarborgen worden omgeven. In dit verband adviseert de Autoriteit, overeenkomstig Aanbeveling 03/2011 van de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de CBPL" genoemd), de wetgever aan te geven dat de kopie van de identiteitskaart moet worden doorgehaald en dat op de kaart moet worden vermeld wie de ontvanger is en welk gebruik de ontvanger ervan mag maken. Zoals de CBPL destijds opmerkte, voorkomt deze procedure dat de identiteitskaart in een getrouwe kopie wordt gereproduceerd en beperkt zij het gebruik ervan voor oneigenlijke doeleinden. Aanbeveling van de Commissie uit eigen beweging nr. 03/2011 over het nemen van een kopie van de identiteitskaart en over het gebruik en de elektronische lezing ervan, blz. 21.

computersystemen van de operator of onderneming die een identificatiedienst aanbiedt, en hen te verbieden kopieën van identiteitsdocumenten te maken.

4. Over de bewaartermijn van identificatiegegevens en -documenten (artikel 127 § 3, laatste lid)

47. Het nieuwe artikel 127, § 3, laatste lid, bepaalt de **bewaartermijn** van de identificatiegegevens en eventuele kopieën van identificatiedocumenten die zijn verzameld op grond van artikel 127 :**12 maanden na het einde van de elektronische communicatiedienst**. De Autoriteit **neemt hiervan kennis**.

5. Over de verplichting om een betrouwbare identificatie te waarborgen (artikel 127, §4, lid 1 en 2)

48. Het nieuwe artikel 127, § 4, 1ste en 2de lid van de telecomwet verplicht de operator «*om alles in het werk (te stellen) om de **betrouwbaarheid van de identificatie** te garanderen van de abonnee die een natuurlijke persoon is. Hij vergewist zich ervan dat de vergaarde identificatiegegevens overeenstemmen met de gegevens op het identiteitsstuk. Hij controleert* :
- *of het identificatiedocument dat de abonnee ter identificatie voorlegt, het origineel is, leesbaar is en de indruk geeft van authenticiteit*
- *dat de geldigheidsdatum van dat document niet overschreden is;*
- *en dat dit document betrekking heeft op de geïdentificeerde persoon* ».

5.1. inzake de toestemming voor het gebruik van gezichtsherkenning om de betrouwbaarheid van identificatie te waarborgen (artikel 127, §4, derde lid)

49. Om deze betrouwbaarheid te waarborgen, biedt artikel 127, §4, derde lid, de operator of het verkooppunt van de elektronische communicatiedienst de mogelijkheid om «*automatisch een vergelijking(uit te voeren) tussen de biometrische gegevens op de foto van het identiteitsdocument van de abonnee en deze van zijn gezicht* ».

50. Het **amendementsontwerp** voorziet in **bepaalde waarborgen** voor de rechten en vrijheden van de betrokken personen:
- De minister van Telecommunicatie en de minister van Justitie moeten de operator of de onderneming die de methode van vergelijking van de biometrische parameters op de foto van het identiteitsdocument van de abonnee met die van zijn gezicht aanbiedt, toestemming hebben gegeven om deze methode te gebruiken, aangezien deze toestemming« *tot doel (heeft) de*

betrouwbaarheid van deze vergelijking ten behoeve van de autoriteiten na te gaan» (nieuw artikel 127, § 4, lid 3 tot 5)[33].

- De abonnee moet zijn toestemming geven, aangezien de operator krachtens artikel 127, § 4, lid 6, ten minste één alternatieve manier van identificatie moet aanbieden.
- *«De operator en het verkooppunt mogen deze biometrische parameters niet meedelen aan een derde als bedoeld in artikel 4, 10) van de AVG. Zij mogen deze maar verwerken binnen de limieten die nodig zijn om het in het derde lid beoogde doel van gezichtsvergelijking te verwezenlijken [te weten : de betrouwbaarheid te garanderen van de identificatie van de abonnee]* ».

51. Het herstelwetsontwerp voorzag reeds in de mogelijkheid voor de operator of het verkoopkanaal van elektronische communicatiediensten om een gezichtsherkenningsmethode te gebruiken (die tot doel heeft de biometrische parameters op de pasfoto van de abonnee op automatische wijze te vergelijken met die van zijn gezicht). De Autoriteit stelde hierover in haar advies 108/2021 onder overweging 104 «*Het gebruik van gezichtsherkenningstechnieken om abonnees te identificeren gaat verder dan wat nodig is in een democratische samenleving, terwijl er in België andere, veiliger en minder indringende middelen zijn (het gebruik van eID of Itsme) om mensen elektronisch te authentiseren*». In de verantwoording van het amendement verklaart de regering dat zij het advies van de Autoriteit betreffende de bijzonder indringende aard van het gebruik van gezichtsherkenning in het kader van de identificatie van abonnees van elektronische-communicatiediensten niet kan volgen. De regering stelt in de verantwoording bij het amendement dat zij «*van mening (is) dat de gezichtsvergelijking die wordt aangewend voor de identificatie van de eindgebruiker geen indringing vormt in de privacy van de abonnees. De biometrische gegevens zullen immers in de praktijk niet worden bewaard. De regering is van mening dat de verwerking van biometrische gegevens waarin artikel 127 voorziet, minder gevoelig is vanuit privacystandpunt dan gezichtsherkenning of vingerafdrukken, waarmee een smartphone ontgrendeld kan worden, aangezien in het tweede geval de biometrische gegevens bewaard moeten worden. Het is niet toelaatbaar dat de wetgeving strikter*

[33] Hierover zegt de verantwoording van het amendement het volgende: «*De ministeriële machtiging die wordt bepaald om deze identificatiemethode te valideren per geval, heeft enkel betrekking op de vraag of deze methode voldoende betrouwbaar is voor de veiligheidsdiensten (in het bijzonder de politie en de inlichtingen- en veiligheidsdiensten). Deze machtiging heeft niet tot doel een uitspraak te doen over de naleving van de wetgeving die tot doel heeft de privacy van de abonnees te beschermen*». De Autoriteit neemt hier nota van, maar geeft aan dat de vraag of een gezichtsherkenningsmethode "voldoende betrouwbaar" is, wel degelijk valt onder de naleving van de wetgeving ter bescherming van de persoonlijke levenssfeer van abonnees aangezien artikel 5.1.c) en d), van de AVG vereist dat de verwerkte gegevens toereikend en ter zake dienend zijn voor de doeleinden waarvoor zij worden verwerkt, en dat zij accuraat zijn. Voorts merkt de Autoriteit op dat, hoewel de geautomatiseerde vergelijking tussen de biometrische parameters op de foto van iemands identiteitsbewijs en die van zijn gezicht momenteel zeer betrouwbaar kan zijn, is aangetoond dat **gezichtsherkenningssystemen kwetsbaar zijn voor "morphing attacks".** Bij deze aanvallen worden de gezichtsbeelden van twee (of meer) personen gecombineerd (gemorfd) en het resulterende gemorfde gezichtsbeeld wordt vervolgens bij de registratie gepresenteerd als biometrische referentie. Indien het gemorfde beeld wordt aanvaard, is het waarschijnlijk dat alle personen die aan het gemorfde gezichtsbeeld hebben bijgedragen, er met succes mee kunnen worden geïdentificeerd. Morphing-aanvallen vormen dan ook een ernstige bedreiging voor gezichtsherkenningssystemen. Deze kwetsbaarheid creëert een risico van identiteitsfraude. De meest doeltreffende maatregel om dit soort aanvallen tegen te gaan, zou zijn dat de foto op identiteitsdocumenten rechtstreeks wordt genomen door de autoriteit die het identiteitsdocument afgeeft. Het ziet er niet naar uit dat dit voor de korte tot middellange termijn is gepland (zie in dit verband J. Merkle, C. Rathgeb, U. Scherhag, C. Busch, R. Breithaupt: "Face Morphing Detection: Issues and Challenges", in Proceedings International Conference on Biometrics for Borders (ICBB), Frontex, Warsaw, October 9-10, (2019)).

is voor een openbaar doel (identificatie van de abonnee in het kader van artikel 127) dan voor toepassingen van de privésector (bijv. ontgrendelen van een smartphone) ».

52. In de eerste plaats herinnert de Autoriteit eraan dat, anders dan de regering beweert, de verwerking van persoonsgegevens - met name de **geautomatiseerde vergelijking tussen de biometrische parameters op de foto van het identiteitsbewijs van de abonnee en die van zijn of haar gezicht** - duidelijk **een inmenging in het privéleven van abonnees vormt**, ook al worden de biometrische gegevens niet opgeslagen. Deze inmenging is bijzonder belangrijk gezien de gevoelige aard van de verwerkte gegevens en de risico's van identiteitsfraude die uit een inbreuk op dergelijke gegevens voortvloeien[34]. Het gebruik van gezichtsherkenningstechnologie en de daarmee gepaard gaande verwerking van biometrische gegevens **kan namelijk grote risico's inhouden voor de rechten en vrijheden van de betrokkenen**, met name in geval van identiteitsfraude. De Autoriteit herinnert eraan dat **elke inmenging in het recht op bescherming van persoonsgegevens alleen is toegestaan** als daarmee een **rechtmatig doel** wordt nagestreefd, het doel **noodzakelijk** blijkt (d.w.z. er mogen geen minder ingrijpende middelen zijn om het doel te bereiken) en de maatregel **evenredig** is (d.w.z. de maatregel moet een juist evenwicht vinden tussen de betrokken rechten en belangen).

53. Voorts merkt de Autoriteit op dat de **vergelijking die wordt gemaakt met het gebruik van biometrische gegevens om een smartphone te ontgrendelen, misleidend is**. Ten eerste worden, in tegenstelling tot wat in het ontwerp is voorzien, de biometrische gegevens die worden gebruikt om een smartphone te ontgrendelen, bewaard in een enclave en verlaten zij de smartphone niet[35]. Ten tweede slaan smartphones, in tegenstelling tot de foto op de identiteitskaart, niet het volledige beeld van het gezicht van de betrokkene op, maar alleen kenmerkende punten of patronen, een subset van kenmerken die uit het beeld van het gezicht van de betrokkene zijn geëxtraheerd ("template") ; dit vermindert het risico van identiteitsfraude in het geval van een inbreuk op deze gegevens.

54. Ten tweede merkt de Autoriteit op dat, hoewel in de verantwoording van het amendement staat dat «*biometrische gegevens in de praktijk niet zullen worden bewaard*», **het dispositief van het amendement geen formeel verbod bevat op het bewaren van biometrische gegevens na de vergelijking.** Maar zelfs indien een dergelijk verbod inderdaad zou worden opgenomen in het dispositief van het nieuwe artikel 127 § 4 van de telecomwet en de overtreding ervan strafbaar zou

[34] De biometrische parameters op de foto van het identiteitsbewijs van de abonnee zijn in feite gegevens die vallen onder artikel 9 van de AVG, dat in beginsel de verwerking van biometrische gegevens verbiedt, tenzij aan een van de voorwaarden van artikel 9.2 is voldaan. Er zij op gewezen dat het noodzakelijk, maar niet voldoende, is dat aan een van de in artikel 9.2 genoemde voorwaarden wordt voldaan, wil de verwerking van biometrische gegevens toelaatbaar zijn. Er moet echter voor worden gezorgd dat deze verwerking - die een inmenging vormt in het recht op privacy van de betrokkenen - een legitiem doel nastreeft, noodzakelijk is voor en evenredig is met dat doel, en daarnaast in overeenstemming is met de bepalingen van de AVG.

[35] Zie bijvoorbeeld, *https://support.apple.com/en-gb/HT208108*

worden gesteld met een specifieke en aanzienlijke straf, **zou er nog steeds een niet te verwaarlozen risico bestaan** dat, na het **uitlekken van gegevens[36]**, **de foto's** die worden gebruikt bij de vergelijking tussen de biometrische parameters op de foto van het identiteitsbewijs van de abonnee en die van zijn of haar gezicht **in omloop blijven**. Gezien het grote risico voor de rechten en vrijheden (met name in geval van identiteitsfraude) dat uit een dergelijk gegevenslek (en uit de verspreiding van dergelijke foto's) zou voortvloeien, **dient het gebruik van gezichtsherkenning alleen te worden beperkt tot situaties waarin het strikt noodzakelijk en evenredig lijkt**. Welnu, zoals de Autoriteit reeds stelde in haar advies nr.108/2021, **lijkt het gebruik van gezichtstechnologie om de betrouwbaarheid van de op grond van het nieuwe artikel 127 van de telecomwet verzamelde identificatiegegevens te controleren, niet noodzakelijk**. Er zijn immers **andere middelen** voor authenticatie op afstand die **veiliger** zijn dan het gebruik van gezichtsherkenning, namelijk het gebruik van eID[37] en het gebruik van gekwalificeerde "trust service providers" die een gekwalificeerde elektronische handtekeningendienst aanbieden (bv. Itsme). Deze twee instrumenten bieden een hoger veiligheidsniveau[38] dan gezichtsherkenning, **terwijl toch de doelstelling wordt bereikt** om de betrouwbaarheid van de identificatie van de betrokken persoon te waarborgen. Bij de overhandiging van de elektronische identiteitskaart controleert de gemeenteambtenaar of de persoon aan wie hij de elektronische identiteitskaart en de bijbehorende codes overhandigt - en die het gebruik van de afstandsauthenticatiemodules mogelijk maken - wel degelijk de persoon is die de kaart bezit (controle op zicht). **Zolang een alternatieve methode beschikbaar is die minder indringend is** in het recht op bescherming van persoonsgegevens om de betrouwbaarheid van de verzamelde identificatiegegevens te waarborgen, **kan de wetgever het gebruik van gezichtsherkenning niet toestaan[39].** De extra waarborgen in het amendement

---

[36] Of, preciezer gezegd, een inbreuk in verband met persoonsgegevens in de zin van artikel 4.12 van de AVG. Dit risico van gegevenslekken is des te groter omdat, zoals de auteur van het amendement zelf opmerkt, «*de operator doorgaans een beroep zal doen op een of meer onderaannemers voor de invoering van de oplossing van de gezichtsvergelijking*». Bovendien merkt de Autoriteit op dat personen niet kunnen controleren dat hun foto niet wordt opgenomen, zelfs indien in het systeem een formeel verbod is opgenomen, met name omdat gezichtsherkenning gebaseerd is op elektronische middelen waarvan zij de configuratie niet kunnen controleren.

[37] In de verantwoording bij het amendement «A*angezien de wet de operatoren verplicht om hun abonnees op een betrouwbare manier te identificeren ten voordele van de autoriteiten en dat identiteitsfraude moet worden vermeden, is het van fundamenteel belang dat de operatoren in staat worden gesteld om deze taken te vervullen via de meest geschikte en betrouwbare identificatiemethodes die passen binnen de context van elk digitaal kanaal en voor alle doelgroepen. De voorgestelde methode zal bijvoorbeeld verhinderen dat iemand zich kan identificeren met behulp van een gestolen eID of een gestolen paspoort*» (onderstreping toegevoegd). De Autoriteit merkt op dat het gebruik van de eID-kaart de houder ervan in staat stelt zich te authenticeren door middel van een pincode die in beginsel alleen bij de houder bekend is. Anders dan de regering stelt, verhindert het gebruik van de pincode in combinatie met het gebruik van de eID voor de authenticatie van de houder in beginsel dat een persoon zich kan authenticeren met een gestolen eID-kaart, zonder dat gezichtsherkenning nodig is. Bovendien moet elke gestolen of verloren eID-kaart als gestolen of verloren worden gemeld. Deze aangifte kan worden gedaan bij de plaatselijke autoriteit, de politie of de helpdesk van het Rijksregister (in de praktijk " Doc Stop ", die toegankelijk is via internet of een gratis telefoonnummer). Als gevolg van deze verklaring wordt het identiteitsdocument "geblokkeerd" (het wordt opgenomen in de CheckDoc-toepassing) en wordt de pincode van de kaart geblokkeerd.

[38] De kans dat een datalek tot identiteitsfraude leidt, is namelijk kleiner.

[39] In de motivering van het amendement verklaart de auteur (in antwoord op advies nr. 108/2021 van de Autoriteit) «*Het is waar dat de klant altijd kan terugvallen op alternatieve methodes zoals ITSME en de eID reader en ook op alternatieve methodes in andere verkoopkanalen zoals in de fysische winkel. Evenwel zijn deze methodes niet steeds het meest geschikt om een antwoord te bieden in elke digitale context. De identificatie op basis van gezichtsvergelijking is complementair en een noodzakelijke aanvulling voor de reeds bestaande methodes. Zo is het moeilijk in te schatten welke groei de ITSME-methode nog zal kennen. ITSME is gemakkelijk in gebruik maar vereist wel een voorafgaande activatie. Dit is niet het geval bij het gebruik van de biometrische gegevens. Zo zijn de operatoren van oordeel dat klanten niet steeds over ITSME zullen beschikken. Het gebruik van de biometrische gegevens is bovendien een oplossing voor niet-Belgische inwoners zonder Belgische*

brengen hierin geen verandering. De toestemming van de betrokkene kan immers niet volstaan om een onevenredige gegevensverwerking te legitimeren. **Het amendement zal worden herzien om operatoren en verkoopskanalen van elektronische-communicatiediensten niet langer de mogelijkheid te bieden een automatische methode te gebruiken om de biometrische parameters op de foto van het identiteitsbewijs van de abonnee te vergelijken met die op zijn of haar gezicht[40]**.

5.2. Betreffende het gebruik van de pincode van de Belgische elektronische identiteitskaart (artikel 127 § 4, laatste lid)

55. het nieuwe artikel 127, § 4, laatste lid, bepaalt «*Wanneer de abonnee zich aan de hand van een Belgische elektronische identiteitskaart identificeert en de operator de in het derde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast, kan de kan de operator aan de abonnee vragen om de pincode in te tikken*». In het licht van bovenstaande overwegingen **moeten de woorden** «***en de operator de in het derde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast*** » **worden geschrapt** en het **woord "kan" moet worden verangen door het woord "moet"**. Indien het de bedoeling is dat de verzamelde identificatiegegevens betrouwbaar zijn, moet immers **systematisch worden geëist** dat personen die hun elektronische identiteitskaart tonen, zich **authenticeren door middel van de pincode**.

6. Betreffende de lijst van de identificatiedocumenten die worden aanvaard ter identificatie van de abonnee (artikel 127, § 5, eerste lid)

56. Het nieuw artikel 127 § 5, eerste lid van de telecomwet geeft een opsomming van de «*toegestane identificatiedocumenten ter identificatie van de abonnee die een natuurlijke persoon is*». De Autoriteit **neemt kennis van deze lijst**.

7. Betreffende de lijst van de identificatiedocumenten die worden aanvaard ter identificatie van de abonnee (artikel 127, § 5, eerste lid)

elektronische kaart voor buitenlanders of voor buitenlanders op bezoek in België. Voor deze klanten zijn de eID reader en ITSME niet beschikbaar. **De Autoriteit is niet overtuigd door het argument dat, aangezien klanten niet altijd toegang zullen hebben tot Itsme, het gebruik van gezichtsherkenning moet worden toegestaan om de betrouwbaarheid van de verzamelde identificatiegegevens te garanderen.** In de eerste plaats is het duidelijk dat de i**ntroductie van het Covid Safe Ticket (CST)** in het dagelijkse leven van de inwoners van België ertoe heeft geleid dat een **groot deel van de bevolking Itsme op zijn smartphone heeft geïnstalleerd** om de applicatie CovidSafe.BE te installeren en om de certificaten (van vaccinatie, test of herstel) waaruit het CST bestaat. Overigens kan het feit **dat personen die niet in België wonen, Itsme niet kunnen installeren en zich niet met een eID-kaart kunnen authenticeren, geen rechtvaardiging vormen voor het toestaan van de verwerking van gegevens** voor de gehele bevolking, hetgeen niet noodzakelijk en dus onevenredig lijkt. Er zijn immers andere manieren voor deze mensen om zich te identificeren (b.v. door naar een verkooppunt te gaan).

[40] Indien de auteur van het amendement, ondanks bovenstaande overwegingen, het gebruik van gezichtsherkenning als methode om de betrouwbaarheid van de identificatie van abonnees te verifiëren zou handhaven, dringt de Autoriteit er hoe dan ook op aan dat van de operatoren wordt verlangd dat zij een alternatief voor gezichtsherkenning voorleggen dat geen significante bijkomende belemmeringen inhoudt zodat dit alternatief niet kan worden beschouwd als een echt alternatief om het vrije karakter van de toestemming te waarborgen.

57. Het nieuw artikel 127, § 5, derde lid bepaalt «*Wanneer de operator een abonnee identificeert uitgaande van een identificatiedocument, bewaart hij een kopie van dat stuk, behalve als het gaat om de Belgische elektronische identiteitskaart*». Allereerst herinnert de Autoriteit eraan dat **het maken van kopieën van identiteitsdocumenten noodzakelijkerwijs een groot risico inhoudt** voor de rechten en vrijheden van de betrokken personen, gezien de mogelijk ernstige gevolgen van een datalek met betrekking tot deze documenten (identiteitsfraude)[41]. Daarom moet h**et kopiëren van identiteitsdocumenten tot een minimum worden beperkt.** Aangezien er een technologische oplossing bestaat waarmee de gegevens betreffende de burgerlijke identiteit van de natuurlijke persoon elektronisch en op betrouwbare wijze aan de elektronische identiteitskaart kunnen worden ontleend, is het niet nodig een kopie van de identiteitskaart te maken en te bewaren. In dit verband **neemt de Autoriteit nota** van het feit dat het amendement reeds bepaalt dat de Belgen zich in beginsel moeten identificeren aan de hand van hun elektronische identiteitskaart[42] en verbiedt dat een kopie van de Belgische elektronische identiteitskaart wordt bewaard. **Om te voorkomen** dat **de Belgische identiteitskaart wordt gekopieerd**, moet echter een technologische oplossing worden gevonden om ervoor te zorgen dat de identiteitsgegevens van de houder van een elektronische identiteitskaart worden geëxtraheerd om rechtstreeks te worden opgenomen in de databank die de operatoren moeten aanleggen overeenkomstig het nieuwe artikel 127 van de telecomwet. **oor andere identiteitsdocumenten** waarvan de identificatiegegevens niet elektronisch en op betrouwbare wijze kunnen worden geëxtraheerd, bepaalt het amendement dat de operator een kopie van het document moet bewaren. In de verantwoording bij het amendement stelt de regering dat het bewaren van een kopie van deze documenten gerechtvaardigd is omdat «*de operatoren (...) minder vertrouwd (zijn) met de buitenlandse identiteitskaarten en vreemdelingenpassen.* Deze redenering overtuigt de Autoriteit niet van de noodzaak om een kopie van deze identiteitsdocumenten te nemen. Gelet op het aanzienlijke risico van identiteitsdiefstal dat voortvloeit uit de verspreiding van kopieën van identiteitsdocumenten, is het aangewezen om, in plaats van die kopieën te bewaren, **enkel te voorzien in de vermelding** in de gegevensbank - die de operatoren overeenkomstig artikel 127 van de telecomwet aanleggen - van **de identiteitsgegevens die uit de raadpleging van identiteitsdocumenten worden verzameld**. Artikel 127, § 5, lid 3, moet worden geschrapt**[43]**.

---

[41] Zie hiervoor de Aanbeveling uit eigen beweging 03/2011 van 25 mei 2011 van de Commissie voor de bescherming van de persoonlijke levenssfeer (voorganger in rechte van de Autoriteit) over het nemen van een kopie van de identiteitskaart en over het gebruik en de elektronische lezing ervan, terug te vinden op de website van de Autoriteit.

[42] De verantwoording van het amendement zegt hierover het volgende «*In principe moet een Belg zich in België identificeren aan de hand van zijn Belgische elektronische identiteitskaart en niet door middel van zijn internationaal paspoort*». Deze verplichting komt in het dispositief tot uiting in het feit dat de Belgen zich alleen met hun paspoort kunnen identificeren voor elektronische communicatiediensten die worden betaald voordat zij worden verleend. Voor alle "postpaid" diensten zullen de Belgen zich enkel nog kunnen identificeren met hun elektronische identiteitskaart.

[43] Indien de regering echter, ondanks de bovenstaande overwegingen, de verplichting handhaaft om een kopie te bewaren van identiteitsdocumenten die geen Belgische elektronische identiteitskaart zijn, dringt de Autoriteit erop aan dat - overeenkomstig Aanbeveling 3/2011 van de CBPL - in het dispositief van het amendment ten minste wordt bepaald dat de kopie van het identiteitsdocument wordt doorgehaald en dat het doel van de kopie op de kopie wordt vermeld, om elke getrouwe reproductie van de kaart te voorkomen en elk gebruik voor oneigenlijke doeleinden te beperken

8. Betreffende de machtiging om facturen van leveranciers van verschillende producten en andere aanvullende informatie te eisen om de betrouwbaarheid van de identiteit van de abonnee te waarborgen (artikel 127, § 5, 4de en 5de lid)

58. Het nieuwe artikel 127 § 5, 4de en vijfde lid bepaalt: «*Wanneer de abonnee een identificatiedocument zoals bedoeld in het eerste lid ter identificatie voorlegt en de operator niet in staat is om de betrouwbaarheid van de identiteit van de abonnee te garanderen aan de hand van dat document, kan hij aan de abonnee vragen om hem het volgende te verstrekken teneinde de betrouwbaarheid te vergroten:*
    - *de facturen van leveranciers van verschillende producten of diensten, voor de elektronische-communicatiediensten die worden betaald nadat ze werden verstrekt;*
    - *aanvullende informatie.*

    De operator houdt een kopie van deze facturen en informatie bij ».

59. In de verantwoording bij het amendement zegt de auteur het volgende: «*Gezien de moeilijkheid voor de operatoren om de identiteitsstukken op te sporen die zouden vervalst zijn, vragen deze laatsten soms aan de abonnee om hen facturen van erkende nutsbedrijven te bezorgen (bijvoorbeeld water-, gas- of elektriciteitsleveranciers). Een operator heeft er immers commercieel belang bij om zijn abonnee correct te identificeren en om identiteitsfraude te vermijden. Het is belangrijk dat de betrouwbaarheid van de identificatie van de abonnee ten behoeve van de autoriteiten van hetzelfde niveau is als de betrouwbaarheid van deze identificatie voor de commerciële behoeften van de operator*».

60. De Autoriteit merkt op dat **een dergelijke bepaling verder gaat dan wat in een democratische samenleving noodzakelijk is**, aangezien zij leidt tot de toelating van potentieel onevenredige en discriminerende gegevensverwerking.

61. Ten eerste merkt de Autoriteit op dat **de bepaling in haar huidige formulering niet voldoende nauwkeurig en voorspelbaar** is om aan het legaliteitsbeginsel te voldoen. In de bepaling wordt namelijk niet aangegeven onder welke omstandigheden de operator niet in staat is de betrouwbaarheid van de identiteit van de abonnee te garanderen. Wat wordt daarmee bedoeld? Heeft dit betrekking op elke situatie waarin een persoon een identiteitsdocument overlegt waarvoor geen pincode bestaat? Gaat het hier om de situatie waarin de persoon die namens de operator het identiteitsdocument verifieert, subjectief van mening is (maar hoe kan het ook anders als de bepaling geen objectieve criteria geeft ?) dat hij/zij niet in staat is de betrouwbaarheid van de identiteit van de abonnee te garanderen? Wanneer is een persoon in staat de betrouwbaarheid van de identiteit van de abonnee te garanderen? **De ontwerpbepaling bepaalt niet met voldoende voorspelbaar onder welke**

voorwaarden en omstandigheden de verwerking van persoonsgegevens die zij toestaat, mag plaatsvinden.

62. Bovendien is **de informatie** die door de operator kan worden gevraagd, **evenmin** op een **duidelijke en voorspelbare manier gedefinieerd**. Aan de ene kant verwijst het naar «*facturen van leveranciers van verschillende producten of diensten*». Over welke producten en diensten gaat het ? Over hoeveel facturen is er sprake? Aan de andere kant bevat de ontwerpbepaling die spreekt van «*aanvullende informatie*», geen enkele andere precisering. **Het gebrek aan duidelijkheid in de gebruikte termen ondermijnt evenzeer het legaliteitsbeginsel.**

63. Bovendien staat in de ontwerpbepaling dat de operator "kan vragen" (en niet "moet vragen") om aanvullende documentatie indien hij niet in staat is de betrouwbaarheid van de identiteit van de abonnee te garanderen. Welnu, krachtens het legaliteitsbeginsel **is het aan de wetgever** om, met inachtneming van de beginselen van noodzakelijkheid, evenredigheid en non-discriminatie, **de voorwaarden vast te stellen waaronder aanvullende documenten moeten worden verzameld en bewaard om de betrouwbaarheid van de identificatie te waarborgen.** Daarnaast is de verwerking van gegevens om dergelijke aanvullende informatie en documenten te verzamelen en op te slaan teneinde de betrouwbaarheid van de identificatie van de abonnee ten behoeve van de autoriteiten te vergroten, **alleen rechtmatig uit hoofde van artikel 6 van de AVG indien dit noodzakelijk is om een wettelijke verplichting** na te komen waaraan de verwerkingsverantwoordelijke onderworpen is (artikel 6.1. c), van de AVG). Er kan imers geen andere rechtmatigheidsgrondslag krachtens artikel 6 van de AVG worden ingeroepen om de gegevensverwerking in deze context te legitimeren. **Wil er echter sprake zijn van een wettelijke verplichting in de zin van artikel 6.1.c) van de AVG, dan mag de verwerkingsverantwoordelijke** (d.w.z. in dit geval de operatoren[44].

64. Voorts kan het **gebrek aan duidelijkheid** over de omstandigheden waarin de operator andere documenten dan identiteitsdocumenten kan eisen en over **de documenten en informatie die in die context kunnen worden geëist**, l**eiden tot een discriminerende toepassing van de wet.** Het is immers waarschijnlijk dat bepaalde categorieën van de bevolking veel systematischer dan andere om aanvullende informatie worden gevraagd om de betrouwbaarheid van hun identiteitsdocument te staven ; en dit zonder dat dit gerechtvaardigd is en in verhouding staat tot het nagestreefde doel. Evenzo kunnen operatoren voor sommige categorieën van de bevolking "veeleisender" zijn dan voor andere met betrekking tot de documenten en informatie die moeten worden verstrekt om de betrouwbaarheid van hun identificatie te garanderen; en dit eveneens zonder rechtvaardiging. **In de wet zijn namelijk geen garanties opgenomen om een discriminerende behandeling van**

[44] Werkgroep "Artikel 29" over de gegevensbescherming (voorganger van het Europees Comité voor gegevensbescherming, Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, WP 217, 21 april 2014, 217, blz 21-22..

bepaalde categorieën van de bevolking te voorkomen. Het is juist dat de operatoren onderworpen zijn aan de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie, die discriminatie verbiedt bij de toegang tot goederen en diensten en de levering van goederen en diensten aan het publiek. **Het is evenwel van essentieel belang dat de regelgeving die specifiek de verwerking van persoonsgegevens regelt, met name de verwerking die nodig is om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke is onderworpen, zoals hier het geval is, zodanig is opgesteld dat wordt vermeden dat deze gegevensverwerking voor de betrokken natuurlijke personen discriminerende gevolgen kan hebben**.

65. Meer fundamenteel **betwijfelt de Autoriteit de noodzakelijkheid en evenredigheid van** de inmenging in het recht op bescherming van persoonsgegevens, die wordt veroorzaakt door **het verzamelen en bewaren van facturen van leveranciers van verschillende producten of diensten en andere aanvullende informatie om de betrouwbaarheid van de identiteit van de abonnee te waarborgen**[45]. Uit de verantwoording bij het amendement wordt niet duidelijk waarom het noodzakelijk en evenredig is om, naast een identiteitsbewijs, facturen voor goederen of diensten of andere informatie te verlangen om een betrouwbare identificatie te waarborgen. **Gezien de aanzienlijke inmenging die een dergelijke verzameling en bewaring van aanvullende informatie veroorzaakt en de risico's van deze maatregel voor de rechten en vrijheden van de betrokkenen, met name discriminatie, is het echter aan de wetgever om met behulp van feitelijke en concrete elementen aan te tonen dat de beoogde gegevensverwerking wel degelijk noodzakelijk en evenredig is. Maar dit is momenteel niet het geval.**.

66. **In het licht van het bovenstaande worden de leden 4 en 5 van het nieuwe artikel 127, § 5, geschrapt**.

9. Betreffende de delegatie aan de Koning om bepaalde specifieke identificatiemethoden toe te staan (artikel 127, § 5, laatste lid)

67. Het nieuwe artikel 127, §5, laatste lid bepaalt: «*De Koning kan een aantal specifieke, eventueel indirecte, identificatiemethodes toestaan voor personen die over geen enkel van de in het eerste lid bedoelde documenten beschikken».* De Autoriteit **neemt kennis van deze bevoegdheidsdelegatie.** Zij vestigt reeds de aandacht van de Koning op het feit dat **deze identificatiemethoden moeten voldoen aan het noodzakelijkheids- en evenredigheidsbeginsel**.

[45] In dit verband merkt de Autoriteit op dat de bepaling zou kunnen leiden tot een brede verzameling van informatie. Denk maar aan het geval van een volwassene die bij zijn of haar ouders woont en wiens water-, gas- en elektriciteitsrekeningen allemaal op naam van een van de ouders staan. Zal deze persoon, om de betrouwbaarheid van zijn of haar identiteit te waarborgen, niet alleen de genoemde facturen moeten overleggen, maar ook een samenstelling van het gezin?

10. Betreffende de identificatiegegevens die de operatoren moeten bijhouden (artikel 127 § 6)

68. Het nieuwe artikel 127, § 6, van de telecomwet bepaalt de **maximale lijst** van identificatiegegevens alsook de **minimale lijst** van identificatiegegevens die moet worden bijgehouden door de operator die de abonnee identificeert aan de hand van een directe identificatiemethode. **De Autoriteit heeft meerdere opmerkingen over deze twee gegevenslijsten:** een eerste opmerking over het beginsel van de twee lijsten van te bewaren gegevens en meer specifieke opmerkingen over de naleving van het beginsel van minimale gegevensverwerking.

69. Ten eerste herinnert de Autoriteit eraan dat de **rechtmatigheidsgrondslag** van de verwerking die bestaat in de identificatie van abonnees en de opslag van hun identificatiegegevens, wordt gerechtvaardigd door de naleving van een **wettelijke verplichting** waaraan de verwerkingsverantwoordelijke is onderworpen (artikel 6.1.c) van de AVG). Zoals de Autoriteit echter al eerder in haar advies heeft opgemerkt, kan er pas sprake zijn van een wettelijke verplichting uit hoofde van artikel 6.1.c) van de AVG als de **verwerkingsverantwoordelijke** (d.w.z. in dit geval de operatoren) **over geen enkele marge beschikt om te bepalen hoe aan de wettelijke verplichting[46] moet worden voldaan**. **De operatoren de keuze geven om bepaalde identificatiegegevens te bewaren** (zonder hen daartoe te verplichten) **is niet toelaatbaar**, gelet op het feit dat het verzamelen en bewaren van identificatiegegevens slechts rechtmatig is **voor zover de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen** waaraan zij onderworpen zijn. Hieruit volgt dat **de wetgever in één enkele lijst de identificatiegegevens moet bepalen die moeten worden bewaard**, zelfs indien dit betekent dat bepaalde gegevens alleen mogen worden bewaard voor zover zij voor de betrokkene bestaan (bv. het rijksregisternummer). **Het amendement moet dus op dit punt worden aangepast**.

70. Ten tweede, **meer specifieke opmerkingen** over de vraag of de te bewaren gegevens voldoen aan de eis dat die gegevens *«toereikend, ter zake dienend en beperkt moeten zijn tot hetgeen noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt (minimalisering van de gegevensverwerking)* » :

a) Op de maximale lijst mogen de volgende gegevens worden bewaard «*de foto van de abonnee, maar enkel voor andere identiteitsstukken dan de Belgische elektronische identiteitskaart*» (artikel 127 §6, eerste lid, 5°). De Autoriteit herinnert eraan dat, overeenkomstig artikel 6 § 4, van de wet

[46] Werkgroep "Artikel 29" over de gegevensbescherming (voorganger van het Europees Comité voor gegevensbescherming, Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, WP 217, 21 april 2014, 217, blz. 21-22.

van 19 juli 1991 betreffende de bevolkingsregisters, identiteitskaarten, vreemdelingenkaarten en verblijfsdocumenten (hierna "de wet van 19 juli 1991" genoemd), het gebruik van de foto van de houder van een identiteitskaart alleen rechtmatkig «*indien dit gebruik bij of krachtens een wet, decreet of ordonnantie*» is toegestaan. Deze voorwaarde voor het gebruik van de foto van de houder van een identiteitskaart toont aan dat de wetgever van oordeel was dat de verwerking van deze gegevens bijzondere risico's voor de betrokkene meebrengt[47]. De foto op de identiteitskaart - of enig ander identiteitsdocument - is wel degelijk een **biometrisch gegeven,** voor zover het op een specifieke technische manier wordt gebruikt om een natuurlijke persoon te identificeren of op unieke wijze te authenticeren. Overeenkomstig artikel 9 § 2.g), van de AVG zou de verwerking van de foto die in een identiteitsdocument is opgenomen - in het kader van het onderhavig amendement- slechts rechtmatig zijn voor zover zij «*noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene*». Gelet op de risico's voor de rechten en vrijheden van de betrokkenen, **ziet de Autoriteit niet in waarom het verzamelen en bewaren van de foto van de houder van een ander identificatiedocument noodzakelijk en evenredig zou zijn met de nagestreefde doelstelling van algemeen belang.** Bij gebrek aan een toereikende en overtuigende rechtvaardiging ten aanzien van de noodzaak en de evenredigheid van het verzamelen en bewaren van deze gegevens, zullen **deze gegevens derhalve worden geschrapt uit de maximale lijst van gegevens die kunnen (of moeten) worden bewaard.**

b) De Autoriteit merkt op dat het **huisadres, e-mailadres en telefoonnummer** (artikel 127,§ 6, eerste lid, 6°) geen identificatiegegevens zijn, maar **contactgegevens**. Zij **dienen derhalve niet te worden opgenomen in de lijst van identificatiegegevens** die door de operatoren moeten worden bewaard.

c) Het begrip "**openbaar veiligheidsnummer**" (artikel 127 § 6, eerste lid, 8°) **moet gedefinieerd worden.** Indien het gaat om het door de Dienst Vreemdelingenzaken toegekende dossiernummer bedoeld in artikel 2 van het koninklijk besluit van 16 juli 1992 tot vaststelling van de gegevens vermeld in de bevolkingsregisters en het vreemdelingenregister, dient dit te worden vermeld.

[47] In de memorie van toelichting bij het wetsontwerp betreffende diverse bepalingen inzake het Rijksregister en de bevolkingsregisters wordt gesteld « *Het wetsontwerp preciseert daarentegen dat de identiteitskaartfoto verwerkt moet worden zoals het rijksregisternummer en de vingerafdrukken, namelijk dat hij niet het voorwerp mag uitmaken van een verwerking, noch geregistreerd, noch gebruikt mag worden (zie punt 74). Aangezien de foto echter ook rechtstreeks zichtbaar is met het blote oog, zou niet hetzelfde beschermingsprocédé als dat voor de vingerafdrukken gebruikt mogen worden*» (54-3256/001, p. 39).

d) De Autoriteit herinnert eraan dat volgens de jurisprudentie van het voormalige sectoraal comité van het Rijksregister het **rijksregisternummer**, in combinatie met de naam en voornaam, een **nauwkeuriger identificatie mogelijk maakt dan het nummer van de identiteitskaart**. Bovendien heeft de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Gegevensbeschermingsautoriteit, er reeds op gewezen dat het nummer van de identiteitskaart niet geschikt is als identificatiemiddel omdat het niet stabiel is in de tijd. In dit verband is de Autoriteit van oordeel dat indien de operator reeds het rijksregisternummer bijhoudt, hij niet - daarnaast - het nummer van de identiteitskaart kan bijhouden **De lijst zal worden gewijzigd om te specificeren dat het documentnummer alleen kan worden behouden in de situatie waarin de operator nog niet over het rijksregisternummer beschikt**.

e) In de minimale lijst van te bewaren gegevens staat het volgende: «*wanneer de operator zijn abonnee identificeert uitgaande van de gegevens die beschikbaar zijn op zijn Belgische elektronische identiteitskaart: het rijksregisternummer, de naam en voornaam* : (artikel 127 §6, tweede lid, 1ste streepje). Deze elementen maken een zekere identificatie van de abonnee mogelijk. **De Autoriteit is daarom van mening dat alleen deze gegevens door de operatoren mogen worden bewaard overeenkomstig artikel 127 van de telecomwet wanneer de abonnee geïdentificeerd is door middel van een Belgische elektronische identiteitskaart**.

f) **De delegatie aan de Koning door artikel 127, § 6, tweede lid, tweede streepje,** om te bepalen welke gegevens (naast de naam, voornaam en geboortedatum) de operator (minimaal) moet bewaren, is **niet in overeenstemming met het legaliteitsbeginsel**, zoals geïnterpreteerd in arrest nr. 158/2021 van het Grondwettelijk Hof.

71. **De lijst van identificatiegegevens die de operatoren moeten bijhouden, zal worden aangepast om tegemoet te komen aan de verschillende opmerkingen die hierboven zijn gemaakt**.

11. Betreffende de indirecte identificatiemethoden (artikel 127, § 9)

72. Het nieuwe artikel 127 § 9 van de telecomwet bepaalt de **verschillende indirecte methoden** waarmee de operatoren de overheid moeten toelaten hun abonnees te identificeren. Het betreft een identificatie:

(1) door de **bewaring van het IP-adres dat werd gebruikt om de account ter gebruik van de elektronische- communicatiedienst te creëren** en de **IP- bronadressen van de verbinding**, het tijdstempel, alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de toegewezen poorten;

(2) door de vergaring en bewaring van het **telefoonnummer** van de abonnee dat werd toegewezen in het kader van een elektronische- communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren krachtens onderhavig artikel;

(3) in geval van een **onlinebetaling** specifiek voor de intekening op een elektronische-communicatiedienst, door de vergaring en bewaring van het **kenmerk van de betalingsverrichting**, **de naam, de voornaam, de geboorteplaats en -datum** van de abonnee die een natuurlijke persoon is of die handelt voor rekening van een abonnee die een rechtspersoon is teneinde zijn verplichtingen inzake identificatie te vervullen;

(4) in geval van een intekening van een abonnee die in **een gesloten centrum of woonunit verblijft**, op een mobiele elektronische-communicatiedienst verstrekt door middel van een voorafbetaalde kaart, door de vergaring en bewaring van de naam en de voornaam van de abonnee, zijn openbaar veiligheidsnummer en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden;

(5) door de vergaring en bewaring van de gegevens **vastgelegd door de Koning**, voor de elektronische-communicatiediensten voor (1) elektronische-communicatiediensten die occasioneel door abonnees worden gebruikt en waarvoor een methode van directe identificatie aanzienlijke beperkingen met zich meebrengt voor abonnees en operatoren en waarvoor een indirecte identificatiemethode de wettelijk bevoegde instanties in staat stelt de abonnee op betrouwbare wijze te identificeren en voor (2) elektronische-communicatiediensten bepaald door de Koning, die worden aangeboden aan personen die niet beschikken over een van de identiteitsdocumenten bedoeld in het nieuwe artikel 127, § 5.

73. Om te beginnen merkt de Autoriteit, zoals zij reeds in bovengenoemd advies heeft opgemerkt, nogmaals op dat de **kwaliteit van de identificatiegegevens** die door middel van een indirecte identificatiemethode worden verzameld, **onzeker lijkt** en niet garandeert dat de persoon die zal worden geïdentificeerd, de persoon is die daadwerkelijk van de elektronische-communicatiedienst gebruik zal hebben gemaakt. **De Autoriteit dringt erop aan dat de parlementsleden de noodzaak en evenredigheid beoordelen van de inmenging in het recht op bescherming van persoonsgegevens door het verzamelen van gegevens die nodig zijn voor de indirecte identificatie van abonnees in het licht van de onzekerheid over de kwaliteit van dergelijke**

gegevens met het oog op de verwezenlijking van het nagestreefde doel, namelijk te zorgen voor een betrouwbare identificatie van de eindgebruiker.

74. Ten tweede merkt de Autoriteit op dat **sommige indirecte identificatiemethoden nieuw lijken te zijn** (dit is het geval voor de onder (1) en (2) opgesomde methoden), terwijl **andere indirecte identificatiemethoden al werden gebruikt** om de eindgebruiker te identificeren van openbare mobiele elektronische-communicatiediensten die op basis van een voorafbetaalde kaart worden aangeboden (dit is het geval voor de onder (3)[48] en (4)[49] opgesomde methoden). **Het amendement breidt echter de categorieën van autoriteiten uit die deze indirecte identificatiemethoden kunnen gebruiken**. Tot nu toe konden alleen inlichtingendiensten en veiligheidsdiensten een eindgebruiker ondubbelzinnig identificeren[50] aan de hand van de kenmerken van de betalingstransactie[51]. Zoals vermeld in de verantwoording bij het amendement: «*Om te garanderen dat de in het eerste artikel, 3°, bedoelde indirecte identificatiemethode in de praktijk werkt, wordt de mogelijkheid om identificatiegegevens te vorderen van een betalingsdienstenaanbieder,[...] uitgebreid naar de andere Belgische autoriteiten die bevoegd zijn om van de telecomoperator de identiteit van de abonnee te krijgen. Als deze autoriteiten deze identiteit kunnen krijgen vanwege de telecomoperator, dan moeten ze die ook kunnen krijgen vanwege een betalingsdienstenaanbieder (identificatie op basis van de referentie van een banktransactie die bewaard wordt door de operator) volgens dezelfde nadere regels, behalve indien de wetgeving houdende regeling van de autoriteit in andere nadere regels voorziet. Dat geldt ook wanneer de naleving van artikel 127 van de telecomwet gecontroleerd wordt door het BIPT*». De Autoriteit herinnert eraan **dat de noodzaak en evenredigheid van deze uitbreiding moet worden gerechtvaardigd op basis van feitelijke en concrete elementen**.7 De verantwoording van het amendement bevat echter geen enkel feitelijk en concreet element waaruit de noodzaak en de evenredigheid blijkt van de uitbreiding van de categorieën van autoriteiten die toegang kunnen krijgen tot de identiteit van een abonnee van een elektronische-communicatiedienst, terwijl deze uitbreiding de inmenging in het recht op persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens van alle abonnees van elektronische-communicatiediensten vergroot. Deze uitbreiding zal worden opgeheven of de noodzaak en evenredigheid ervan zal worden gerechtvaardigd met feitelijke en concrete elementen.

[48] Zie artikel 17 van het Koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.
[49] Zie het ministerieel besluit waarbij de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken wordt aangewezen als een overheidsinstantie overeenkomstig artikel 9, lid 2, van het Koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.
[50] In de motivering van amendement nr. 16 geeft de regering aan dat artikel 46bis van het WSV dat de rechtsgrondslag vormt op grond waarvan de procureur des Konings kan overgaan tot de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst, reeds een rechtsgrondslag biedt voor indirecte identificatie op grond van artikel 127 van de wet op de elektronische communicatie maar dat hij van mening is dat deze mogelijkheid nader moet worden gepreciseerd in de organieke wetten van de autoriteiten die van deze identificatiemethoden gebruik wensen te maken. Artikel 46bis van het wetboek van Strafvordering moet dus worden gewijzigd. De Autoriteit merkt op dat uit een lezing van artikel 46bis van het WSV niet duidelijk blijkt dat de procureur des Konings bevoegd is om financiële instellingen te verplichten de identiteit bekend te maken van de persoon "achter" de referentie van een elektronische banktransactie.
[51] Deze methode is namelijk opgenomen in artikel 16/2 van de organieke wet van 30 november 1998 betreffende de inlichtingen- en veiligheidsdiensten.

75. Daarnaast heeft de Autoriteit **meerdere opmerkingen** over de gegevens die zijn verzameld in het kader van de indirecte identificatiemethoden.

76. Ten eerste merkt de Autoriteit met betrekking tot het verzamelen van gegevens in geval van online elektronische betaling op dat het verzamelen van geboortedatum en -plaats verder gaat dan wat nodig is om het doel van indirecte identificatie te verwezenlijken en derhalve in strijd is met artikel 5.1.c) van de AVG. **Het amendement zal worden herzien om de verplichting tot het verzamelen van deze twee gegevens te schrappen**.

77. Vervolgens over het **verzamelen van IP-adressen als indirecte identificatiemethode** :

- Ten eerste merkt de Autoriteit op dat **het verzamelen en bewaren van het IP-adres dat wordt gebruikt voor het aanmaken van de account** die het gebruik van de elektronische-communicatiedienst mogelijk maakt, **al krachtens het nieuwe artikel 126 § 1, 4°** (ingevoerd bij amendement 1), voor dezelfde periode **moet worden verzameld en bewaard**. De Autoriteit vraagt zich daarom af waarom dezelfde gegevens krachtens artikel 127 moeten worden verzameld.

- Ten tweede merkt de Autoriteit op dat het voor een gebruiker betrekkelijk eenvoudig is om deze indirecte identificatiemethode te omzeilen, bijvoorbeeld door zich te abonneren op of gebruik te maken van de elektronische-communicatiedienst via een openbaar of open wifi-netwerk of door Tor te gebruiken. Onder deze omstandigheden is de Autoriteit van mening dat het verzamelen en bewaren van het IP-adres dat is gebruikt om de account aan te maken en de IP-adressen die zijn toegewezen aan de bron van de verbinding het niet systematisch mogelijk maken het nagestreefde doel op adequate wijze te bereiken. De Autoriteit betwijfelt derhalve of de maatregel passend (en derhalve noodzakelijk) is. De Autoriteit verzoekt de parlementsleden te beoordelen - en zo nodig te motiveren - of de maatregel inderdaad relevant en noodzakelijk is voor het bereiken van de doelstelling die zij wensen na te streven.

- Ten derde vraagt **de Autoriteit zich af of het verzamelen en bewaren van IP-adressen aan de bron van de verbinding tot doel heeft de verzameling en bewaring te eisen van alle IP-adressen die gebruik maken van de elektronische-communicatiedienst.** Indien dit het geval is, zou het amendement de operatoren **opleggen om algemene en niet-gedifferentieerde verkeersgegevens te bewaren**, namelijk de IP-adressen van apparatuur die verbinding maakt met een elektronische-communicatiedienst ; die een inmenging zou vormen in het recht op persoonlijke levenssfeer van de betrokken personen die volgens de Autoriteit **als significant moet worden aangemerkt**, met name omdat zij het mogelijk maakt de gebruiksfrequentie van een elektronische-communicatiedienst te bepalen (hetgeen verder gaat

dan de vraag wie zich op die dienst abonneert) en informatie af te leiden over de plaats waar de gebruiker van de dienst zich bevindt (met name wanneer het berichtendiensten betreft)[52]. De Autoriteit merkt voorts op dat **krachtens artikel 127 verzamelde gegevens**, en dus IP-adressen die zijn toegewezen aan de bron van de verbinding met behulp van een elektronische-communicatiedienst, **tot twaalf maanden na het einde van het contract moeten worden bewaard** (zie nieuw artikel 127, § 3, lid 3). **Een dergelijke bewaartermijn** voor alle IP-adressen die verbinding hebben gemaakt met een elektronische-communicatiedienst **is buitensporig en onevenredig. Het amendement moet worden aangepast** om **de bewaartermijn** voor IP-adressen die verbinding maken met een elektronische-communicatiedienst te beperken, zoals bepaald in het nieuwe artikel 126 van de telecomwet, en niet tot 12 maanden na het einde van de dienst.

- Tot slot **vraagt de Autoriteit zich meer in het algemeen af** of het **relevant is om het IP-adres dat is gebruikt om de account aan te maken en de IP-adressen die aan de bron van de verbinding zijn toegewezen, ook na twaalf maanden na het einde van de sessie te bewaren** met het oog op de identificatie van abonnees op een gratis elektronische-communicatiedienst, aangezien het twaalf maanden na het einde van de sessie blijkbaar niet meer mogelijk is om de persoon te identificeren aan wie het IP-adres dat is gebruikt om de account aan te maken of het IP-adres dat is gebruikt om verbinding te maken met de elektronische-communicatiedienst, is toegewezen. Internetproviders, die IP-adressen toewijzen, moeten de IP-adressen die aan de bron van een verbinding zijn toegewezen immers nog 12 maanden na het einde van de sessie bewaren. Indien een persoon zich abonneert op een gratis elektronische-communicatiedienst via het internet, zal de operator van die dienst het IP-adres bewaren van waaruit de account (of alle IP-adressen die op die dienst zijn aangesloten) is aangemaakt; dit is om te voldoen aan zijn verplichting om al zijn abonnees te identificeren - of ten minste de identificatie door de autoriteiten mogelijk te maken. Om deze persoon daadwerkelijk te kunnen identificeren, zullen de autoriteiten echter niet alleen het IP-adres dat is gebruikt om de account aan te maken of verbinding te maken met de elektronische-communicatiedienst, bij de operator van die dienst moeten opvragen, maar zullen zij vervolgens de internetprovider moeten vragen naar de identiteit van de abonnee aan wie dit IP-adres was toegewezen op het moment dat de account werd aangemaakt of de dienst werd gebruikt. Indien de toewijzing echter meer dan 12 maanden geleden heeft plaatsgevonden, zal de internetprovider geen toegang meer hebben tot deze informatie en zullen de autoriteiten er niet van op de hoogte zijn. Onder deze omstandigheden, en gezien de ernst van de inmenging die wordt veroorzaakt door het algemeen

[52] Er bestaan immers verschillende technieken waarmee de locatie van de eindapparatuur waaraan dit IP-adres is toegewezen (en dus de locatie van de gebruiker ervan) uit een IP-adres kan worden afgeleid. Er zijn op het internet zelfs diensten beschikbaar die een apparaat (en de persoon die het gebruikt) kunnen lokaliseren op basis van het IP-adres (zie bijvoorbeeld https://www.ip2location.com, /https://iplocation.com/, https://www.home.neustar/resources/tools/ip-geolocation-lookup-tool). De grote spelers, zoals Google of Apple, kennen de locatie van veel IP-adressen (alle mobiele apparaten met locatiediensten) en kunnen andere IP-adressen lokaliseren als zij informatie hebben over de Wi-Fi-SSID's of BLE-tags die het apparaat kan zien.

bewaren van IP-adressen, is de Autoriteit van mening dat het amendement moet worden gewijzigd om te specificeren dat de IP-adressen die worden gebruikt om de account aan te maken en de IP-adressen die worden toegewezen aan de bron van de verbinding, die worden gebruikt als een methode voor indirecte identificatie, **moeten worden bewaard tot twaalf maanden na het einde van de sessie** (en niet twaalf maanden na het einde van de dienst)

12. Betreffende het weerlegbare vermoeden dat de abonnee van een elektronische-communicatiedienst wordt geacht deze dienst zelf te gebruiken (artikel 127, § 10, eerste lid)

78. Het nieuwe artikel 127, § 10, eerste lid, stelt een **weerlegbaar vermoeden** in dat «*de geïdentificeerde persoon geacht (wordt) zelf de elektronische-communicatiedienst te gebruiken*». Zoals de Autoriteit eerder in haar advies heeft opgemerkt, **is het in de praktijk niet ongebruikelijk dat de gebruiker van een elektronische-communicatiedienst verschilt van de persoon die zich op die dienst heeft geabonneerd**: abonnees kunnen een andere persoon machtigen om gebruik te maken van een elektronische-communicatiedienst waarop zij zich hebben geabonneerd (met name een internettoegangsdienst of een vaste of mobiele telefoondienst). Elektronische communicatiediensten, met name die van het type "OTT", kunnen worden **gehackt zonder dat de betrokkene daarvan op de hoogte is**. Een wifi-netwerk kan ook worden gehackt of gedeeld door meerdere gebruikers (met name in het geval van een "open" wifi-netwerk of het aanbieden van een wifi-netwerk in een café). Anderzijds kan iemand zijn of haar mobiele telefoon verliezen of laten stelen en dit pas enkele dagen na de gebeurtenis beseffen. De wetgever kan er immers niet van uitgaan dat de eigenaar van een simkaart te allen tijde weet waar die simkaart zich bevindt. In tegenstelling tot de identiteitskaart[53] is **er geen wettelijke verplichting om de SIM-kaart(en) die men bezit bij zich te dragen**. Hoewel het vermoeden weerlegbaar is en door de betrokkene op enigerlei wijze kan worden betwist, moet er rekening mee worden gehouden **dat het uiterst moeilijk, zo niet onmogelijk, kan zijn om negatief bewijs te leveren** (namelijk dat de geïdentificeerde persoon niet degene is die de elektronische-communicatiedienst heeft gebruikt). **De Autoriteit verzoekt parlementsleden dan ook om uiterst voorzichtig te zijn alvorens een dergelijk vermoeden in het positief recht te handhaven (en uit te breiden)**.

[53] Artikel 6, § 7, van de wet van 19 juli 1991 en artikel 1 van het koninklijk besluit van 25 februari 2003 betreffende de identiteitskaarten.

13. betreffende de voorwaarden waaronder een rechtspersoon zich namens en voor rekening van natuurlijke personen die abonnees zijn op een elektronische-communicatiedienst kan abonneren (artikel 127, § 10, lid 2)

79. Het nieuwe artikel 127, §10, tweede lid, bepaalt onder welke voorwaarden een rechtspersoon zich namens en voor rekening van natuurlijke personen die abonnees zijn, op een elektronische-communicatiedienst kan abonneren.

80. De eerste voorwaarde is dat de rechtspersoon zich overeenkomstig het nieuwe artikel 127, § 7, bij de operator identificeert. De Autoriteit **neemt hiervan akte.**.

81. De tweede en derde voorwaarde bestaan erin dat de rechtspersoon «*een geactualiseerde lijst bewaart aan de hand waarvan het verband kan worden vastgesteld tussen de elektronische-communicatiedienst en de abonnees, met daarin ten minste de naam, de voornaam en het rijksregisternummer van de abonnee*» en « *hij de abonnees identificeert aan de hand van een van de identiteitsstukken bedoeld in paragraaf 5 [dat een lijst bevat van identiteitsdocumenten aan de hand waarvan een persoon kan worden geïdentificeerd], conform de vereisten inzake betrouwbaarheid bedoeld in paragraaf 4, eerste en tweede lid*». **De Autoriteit neemt kennis van deze twee verplichtingen** voor rechtspersonen die zich namens een natuurlijke persoon abonneren op een elektronische-communicatiedienst.

82. De vierde verplichting bestaat uit het verstrekken aan «*de operator (van) een kopie van het identificatiedocument van de abonnees, behalve wanneer het gaat om de Belgische elektronische identiteitskaart, conform paragraaf 5, derde lid*». **Om dezelfde redenen als die welke werden aangevoerd bij de beoordeling van artikel 127, § 5, 3de lid, is de Autoriteit van mening dat deze vierde verplichting moet worden geschrapt**.

83. Het nieuwe artikel 127, § 10, derde lid, bepaalt de termijn waarbinnen de rechtspersoon de gegevens betreffende een abonnee in de bijgewerkte lijst moet bewaren: 12 maanden na het einde van de elektronische-communicatiedienst. **De Autoriteit neemt hiervan kennis**.

14. Betreffende de verplichting om het chassisnummer te bewaren van het voertuig waarin een van de SIM-kaarten of een gelijkwaardige kaart is ingebouwd (artikel 127, § 10, 3de lid)

84. Het **nieuwe artikel 127 § 10, 5de lid** verplicht de operator om «*het chassisnummer van het voertuig waarin een van zijn simkaarten ("subscriber identity/identification module") of een gelijkwaardige kaart werd ingebouwd, evenals de link tussen het chassisnummer en het nummer van deze kaart, vanaf de*

activeringsdatum van de elektronische- communicatiedienst tot twaalf maanden na de stopzetting van de dienst». aangezien «*De Koning nadere bepalingen van de verplichting bedoeld in het derde lid (kan) vastleggen en de ondernemingen die over het chassisnummer beschikken, (kan) verplichten om dat door te geven aan de operatoren*».

85. Deze **nieuwe verplichting** voor operatoren om gegevens te bewaren wordt **als volgt gerechtvaardigd**: *«Uit de evolutie blijkt dat het (meer en meer) moeilijk is voor de autoriteiten om zich in hun onderzoeken de elektronische-communicatiediensten ten nutte te maken. In sommige gevallen slaagt een abonnee erin om zich onder een valse identiteit bij de operator te identificeren. De jurisprudentie van het HvJ-EU heeft de mogelijkheid om de operatoren ertoe te verplichten op algemene en ongedifferentieerde wijze metagegevens te bewaren, sterk ingeperkt. Het is steeds moeilijker voor de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten om toegang te krijgen tot de inhoud van de communicatie, gelet op de invoering van 5G en de veralgemening van eind-tot-eindencryptie. Het is dus van fundamenteel belang dat de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten voordeel kunnen halen uit de nieuwe kansen die door de evolutie van de technologieën worden geboden. In dat kader is net bepaald dat de operatoren de nummers van simkaarten die geïntegreerd zijn in geconnecteerde voertuigen bewaard moeten worden door de link te leggen met het chassisnummer van die voertuigen. Deze verplichting concretiseert een voorstel van de operatoren zelf. De identificatie van de maatschappij waarmee de operator een contract heeft gesloten (de abonnee) zal niet volstaan voor de veiligheidsdiensten, die zullen proberen de identiteit te achterhalen van de natuurlijke persoon of rechtspersoon die de eigenaar van het voertuig is alsook de identiteit van de hoofdbestuurder van het voertuig* ».

86. De Autoriteit benadrukt dat deze nieuwe verplichting voor operatoren om gegevens te bewaren een inmenging vormt in het recht op bescherming van persoonsgegevens die, om toelaatbaar te zijn, een doelstelling van legitiem belang moet nastreven en noodzakelijk en evenredig met die doelstelling moet zijn. De rechtvaardiging die de regering aanvoert, overtuigt de Autoriteit niet van de noodzaak en de evenredigheid van de maatregel. De Autoriteit merkt tevens op dat het risico bestaat dat dergelijke gegevens door operatoren voor andere doeleinden worden gebruikt. **Ofwel kan de regering met feitelijk en concreet bewijs aantonen dat het inderdaad noodzakelijk en evenredig is om het chassisnummer van het voertuig waarin een van de SIM-kaarten of een gelijkwaardige kaart is ingebouwd te bewaren, alsmede het verband tussen het chassisnummer en het nummer van deze kaart, en moet deze motivering worden opgenomen in de verantwoordig van het voorgestelde amendement, ofwel kan de regering dit bewijs niet leveren en wordt deze bepaling geschrapt.**

E. Betreffende amendement nr. 7

87. Amendement nr. 7, dat ertoe strekt een **nieuw artikel 127/4** in de telecomwet in te voegen om een verbod op te nemen dat voordien was opgenomen in artikel 127, § 2, van de Telecomwet, voorziet in een verbod op de levering of het gebruik van een dienst of uitrusting die de volgende verrichtingen verhindert:
1° noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn en de verstrekking van de identificatiegegevens van de oproeper;
2° de identificatie van de eindgebruiker, het opsporen en lokaliseren van privécommunicatie onder de voorwaarden bepaald door de wet;
3° het afluisteren, kennisnemen en opnemen van privécommunicatie onder de voorwaarden bepaald door het Wetboek van Strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

88. **Zoals de Autoriteit reeds in overweging 162 van haar advies nr. 108/2021** heeft opgemerkt, leidt het verbod op het gebruik van systemen die de identificatie van de eindgebruiker, het traceren en lokaliseren van niet openbaar beschikbare communicatie en het bewaren van identificatie-, verkeers- of locatiegegevens kunnen verhinderen, tot de onwettigheid van diensten als Tor, cmix en nym, die een anoniem gebruik van het internet mogelijk moeten maken[54]. Een dergelijk algemeen verbod **is een onevenredige aantasting van het recht op eerbiediging van het privéleven van de betrokkenen, en gaat dus verder dan wat in een democratische samenleving noodzakelijk is.** Dit verbod moet dus worden geschrapt.

F. Betreffende amendement nr. 12

89. Amendement nr. 12 heeft tot doel de **voorwaarden vast te stellen waaronder het BIPT** toegang kan krijgen:

- tot «*gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst*»,d.w.z. de gegevens aan de hand waarvan de burgerlijke identiteit van de abonnee die een natuurlijke persoon is of de gewoonlijke gebruiker van de dienst of de identiteit van de abonnee die een rechtspersoon is, kan worden vastgesteld (nieuw artikel 15, § 1, van de wet BIPT).

- tot «*andere elektronische-communicatiemetagegevens verstrekt dan de gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst*», d.w.z. andere verkeers- en locatiegegevens

[54] De Autoriteit merkt op dat Tor inderdaad kan worden gebruikt door personen die misdrijven willen plegen, maar ook door personen die de grondrechten verdedigen, door journalisten, door organisaties van de civiele samenleving en zelfs door overheidsdiensten (politie, inlichtingendiensten, enz.). Uit de lijst van Tor-sponsors blijkt dat het netwerk niet alleen een "vertegenwoordiging van criminelen" is, maar ook nuttig is voor maatschappelijke organisaties en overheidsdiensten (zie https://www.torproject.org/about/sponsors).

dan die waarmee de abonnee of de gewoonlijke gebruiker van de dienst kan worden geïdentificeerd (nieuw artikel 15 § 2 van de Wet BIPT).

- de gegevensbanken van de operatoren ter uitvoering van de artikelen 122 tot 127 van de telecomwet, met het oog op het toezicht op de naleving van deze artikelen en hun uitvoeringsbesluiten (nieuw artikel 15 § 3 van de wet BIPT).

90. De Autoriteit herinnert eraan dat zij zich in **haar Advies nr. 32/2022** (zie met name de overwegingen 58 e.v.) heeft uitgesproken over bepaalde aspecten van een soortgelijke bepaling als die welke in dit advies aan de orde is. **De Autoriteit verwijst naar dit advies voor de aspecten die in voorliggend advies niet aan bod komen**.

1. Betreffende de noodzaak voor het BIPT om toegang te hebben tot de identificatiegegevens van abonnees en gewoonlijke gebruikers van elektronische-communicatiediensten en metagegevens over de communicatie

91. Het nieuwe artikel 15, §§ 1 en 2, van de wet op het BIPT bepaalt de doeleinden waarvoor het BIPT toegang kan krijgen tot de gegevens die door de operatoren worden bijgehouden. De bepalingen van artikel 14, § 1, 3°, a) en g) tot en met i), van de wet BIPT moeten worden toegepast en gecontroleerd, namelijk :
    - de wet van 13 juni 2005 betreffende de elektronische communicatie;
    - de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren voor de sectoren elektronische communicatie en digitale infrastructuur;
    - 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 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.

92. Zoals de Autoriteit reeds heeft opgemerkt in haar advies nr. 32/2022, **is het aan de wetgever om zich ervan te vergewissen dat het inderdaad noodzakelijk is dat het BIPT toegang heeft tot de gegevens waarmee de abonnee of de gebruikelijke gebruiker van de dienst kan worden geïdentificeerd en tot de onbewerkte communicatiemetadata** met name door na te gaan of het BIPT niet in staat is zijn taken uit te voeren indien het geen toegang heeft tot de communicatiemetadata. De Autoriteit benadrukt met name dat, **indien het mogelijk is dat het BIPT alle of sommige van de hierboven opgesomde taken uitvoert met behulp van geanonimiseerde of gepseudonimiseerde gegevens**, het ontwerp moet bepalen dat alleen geanonimiseerde of gepseudonimiseerde gegevens aan hen kunnen worden doorgegeven. **Dit**

onderzoek moet grondig gebeuren, opdracht per opdracht[55]. Uit de verantwoording van het amendement blijkt niet dat de regering dit onderzoek daadwerkelijk heeft uitgevoerd.

93. Net als in zijn advies nr. 32/2022 herinnert de Autoriteit eraan dat indien **en voor zover het BIPT een openbaredienstopdracht heeft om cyberaanvallen in realtime op te sporen en te stoppen** (wat kan inhouden dat bepaalde diensten of IP-adressen moeten worden geblokkeerd om bijvoorbeeld DDOS-aanvallen te stoppen, botnets uit te schakelen of phishing-pogingen te stoppen), **begrijpt de Autoriteit dat het BIPT toegang moet kunnen krijgen tot onbewerkte metadata van elektronische communicatie**. Gezien de ernst van de inmenging die deze toegang in het recht op privacy veroorzaakt, acht de Autoriteit het echter van **essentieel belang dat er een diepgaand parlementair debat wordt gehouden om de exacte contouren te bepalen van de bevoegdheden en taken** van de politie, de justitiële diensten, de inlichtingendiensten, de militaire diensten of de bestuurlijke autoriteiten die verantwoordelijk zijn voor 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 verwerking van metagegevens (bijvoorbeeld door inlichtingendiensten en politiediensten) die zijn verzameld in het kader van de bestrijding van cybercriminaliteit.

2. Betre de toegang van het BIPT tot de identificatiegegevens van abonnees en regelmatige gebruikers

94. Het **nieuwe artikel 15, § 1** van de wet op het BIPT heeft betrekking op de toegang tot «*gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst*» wanneer dit noodzakelijk is voor de vervulling van een van de in de wet op het BIPT opgesomde taken. Het BIPT kan een schriftelijk en gemotiveerd verzoek formuleren, rechtstreeks aan de operator, die verplicht is het te beantwoorden. Het nieuwe artikel 15, § 5, preciseert dat de motivering betrekking moet hebben op het verband tussen de gevraagde gegevens en de opdracht van het BIPT en op het strikt noodzakelijke karakter van de gevraagde gegevens in het kader van de opdracht. Er is geen voorafgaande controle voorzien.

95. **Ervan uitgaande dat het BIPT inderdaad toegang moet hebben** tot de identificatiegegevens van abonnees of gewoonlijke gebruikers van elektronische-communicatiediensten voor de uitvoering van (een deel van) zijn taken - hetgeen de wetgever moet nagaan -, zijn **de modaliteiten van deze toegang** tot de identificatiegegevens van abonnees of gewoonlijke gebruikers van elektronische-

[55] De Autoriteit wijst er echter op dat het bijzonder moeilijk kan zijn om metagegevens betreffende elektronische communicatie effectief 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 metadata van de elektronische communicatie. Zie Ana-Maria Creţu, Federico Monti, Stefano Marrone, Xiaowen Dong, Michael Bronstein, Yves-Alexandre de Montjoye, "Interaction data are identifiable even across longperiods of time", *Nature Communications*, 25 januari 2022.

communicatiediensten **in overeenstemming met de vereisten die het Grondwettelijk Hof heeft vastgesteld in zijn arrest nr.158/2021**. De Autoriteit **neemt hiervan kennis.**.

3. Betreffende de toegang van het BIPT tot de metagegevens van elektronische communicatie

96. Het nieuwe artikel 15, § 2 handelt over «*de toegang tot andere elektronische-communicatiemetagegevens verstrekt dan de gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst*». **De toegang tot deze gegevens** is, behalve in naar behoren gemotiveerde dringende gevallen, **onderworpen aan de voorafgaande schriftelijke toestemming van de Autoriteit**, die aldus met een nieuwe taak wordt belast.

3.1. Betreffende de categorieën metagegevens waartoe het BIPT toegang kan krijgen

97. De Autoriteit merkt om te beginnen op dat **niet wordt verduidelijkt tot welke metadata** over elektronische communicatie **het BIPT toegang kan hebben.** De ontwerpbepaling is zeer ruim geformuleerd en biedt het BIPT a priori de mogelijkheid om toegang te vragen tot alle gegevens die door de operatoren worden bijgehouden, met inbegrip van de gegevens die worden bijgehouden ter uitvoering van het nieuwe artikel 126/1 van de telecomwet dat - ter herinnering - de operatoren verplicht om in principe **gedurende 12 maanden**[56] de **verkeers- en locatiegegevens te bewaren van alle communicaties vanuit** of **naar** een van de **geografische gebieden** die het artikel opsomt. Gelet op de **bijzonder ernstige inmenging** als gevolg van de bewaring van gegevens op grond van het nieuwe artikel 126/1 van de telecomwet, vereist het evenredigheidsbeginsel, zoals uitgelegd door het HvJEU, echter dat toegang tot dergelijke gegevens alleen mag worden verleend om een van de in artikel 15 van de e-privacyrichtlijn genoemde doelstellingen na te streven, die van bijzonder groot belang is. **De Autoriteit stelt vast dat de auteur van het amendement niet motiveert waarom de door het BIPT uitgevoerde taken (waarvoor het BIPT toegang kan vragen tot metagegevens over communicatie) zo belangrijk zijn dat dit een bijzonder ernstige inmenging van de rechten en vrijheden van de betrokken personen kan rechtvaardigen**.

98. **Bij gebrek aan een gemotiveerde rechtvaardiging van het belang van het nagestreefde doel (in het licht van de door het HvJEU benadrukte vereisten), zal de ontwerpbepaling moeten worden gewijzigd om de mogelijkheid uit te sluiten dat het BIPT toegang vraagt tot de gegevens die worden bewaard ter uitvoering van artikel 126/1 van de telecomwet**.

[56] Tenzij een andere duur zou worden voorzien in dit nieuwe artikel 126/1 van de telecomwet. Deze bepaling voorziet in bepaalde omstandigheden in kortere bewaartermijnen. Zie het nieuwe artikel 126/1 §3, 1° van de telecomwet.

99. Bovendien, en meer in het algemeen, merkt de Autoriteit op dat het vereiste van voorspelbaarheid, gekoppeld aan het beginsel van de minimale gegevensverwerking dat is vastgelegd in artikel 5, § 1, c), van de AVG, vereist dat in de ontwerpbepaling **precies wordt afgebakend tot welke categorieën gegevens het BIPT toegang kan hebben om welke taken te vervullen**. Met andere woorden, de ontwerpbepaling moet voor elke taak van het BIPT de categorieën gegevens vaststellen waartoe deze instelling toegang moet hebben om de haar toevertrouwde taken van openbare dienstverlening te vervullen, aangezien deze categorieën gegevens «*toereikend, ter zake dienend en beperkt moeten zijn tot hetgeen noodzakelijk is gelet op de doeleinden waarvoor zij worden verwerkt* ».

3.2. Betreffende de modaliteiten van de controle voorafgaand aan de toegang tot de metagegevens door het BIPT

100. In haar advies **nr. 32/2022** heeft de Autoriteit zich reeds uitgesproken over **de modaliteiten van de voorafgaande controle** die wordt overwogen voor de toegang tot metagegevens van elektronische communicatie door het BIPT.

101. De Autoriteit heeft ook uitvoerig stilgestaan bij **de nieuwe bevoegdheid van de GBA inzake voorafgaande toestemming in de bijlage bij het advies over een wetsontwerp tot wijziging van de wet tot oprichting van de gegevensbeschermingsautoriteit**.[57]**,**

102. **De Autoriteit verwijst hiernaar en dringt erop aan dat naar behoren rekening wordt gehouden met de opmerkingen in de overwegingen 66-73 van advies nr. 32/2022 en de overwegingen 59-64 van de bijlage bij het advies over het wetsontwerp tot wijziging van de wet tot oprichting van de GBA**.

4. Betreffende de nadere regels voor de raadpleging van gegevensbanken ter uitvoering van de artikelen 122, 123, 126, 126/1, 126/2 en 127 van de telecomwet

103. Het nieuwe artikel 15, § 3, van de wet betreffende het BIPT verwijst naar de specifieke situatie waarin het BIPT optreedt als toezichthoudende autoriteit voor de nationale bepalingen die ter uitvoering van de e-privacyrichtlijn zijn vastgesteld. De ontwerpbepaling voorziet in de modaliteiten waarin het BIPT de gegevensbanken ter uitvoering van de artikelen 122, 123, 126, 126/1, 126/2 en 127 van de telecomwet kan raadplegen, teneinde de naleving van deze bepalingen door een operator te

[57] beschikbaar op https://www.autoriteprotectiondonnees.be/publications/annexe-avis-sur-lavant-projet-de-loi-portant-modification-de-la-loi-apd.pd

controleren. **De Autoriteit neemt nota van deze regelingen, die geen aanleiding geven tot enig commentaar van haar kant**.

G. Betreffende amendement nr. 15

104. Het amendement nr. 15 beoogt **een nieuw artikel 25/1 in de BIPT-wet** in te voegen.

105. Het **nieuwe artikel 25/1, § 1** van de wet betreffende het BIPT heeft tot doel de officier van gerechtelijke politie van het BIPT toe te staan om, op basis van een schriftelijk en gemotiveerd verzoek, informatie op te vragen die hem in staat stelt **de abonnee of de gewoonlijke gebruiker** van een elektronische-communicatiedienst te identificeren, met het oog op het **onderzoek, de vaststelling of de vervolging van een inbreuk** bedoeld in artikel 145, § 3 of § 3bis van de telecomwet of in artikel 24, § 1, 2° van de wet betreffende het BIPT.

106. Met het oog op deze identificatie kan de officier van gerechtelijke politie van de operator verlangen dat hij hem de gegevens met betrekking tot de abonnee of de gewoonlijke gebruiker van de dienst verstrekt die voor dit doel noodzakelijk zijn. De officier van gerechtelijke politie kan ook om de samenwerking verzoeken :
(1) banken en financiële instellingen (ingeval operatoren de referentie van een elektronische bankverrichting meedelen),
(2) gesloten centra en woonunits voor buitenlanders (waar de inschrijving van de abonnee op een elektronische- communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaand meegedeeld zijn door een operator), of
(3) andere rechtspersonen die de abonnee zijn van een operator, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaand meegedeeld zijn door een operator.

107. Het nieuwe artikel 25/1, § 5, preciseert dat de redenen voor het verzoek om identificatie betrekking moeten hebben op (1) het verband tussen de gevraagde gegevens en het doel van het onderzoek, de vaststelling of de vervolging van het specifieke strafbare feit dat het verzoek rechtvaardigt en (2) de strikt noodzakelijke aard van de gevraagde gegevens in het kader van het onderzoek. Er is geen voorafgaande controle voorzien.

108. Wat betreft de bevoegdheid van de officier van gerechtelijke politie om abonnees en gewoonlijke gebruikers van een elektronische-communicatiedienst te identificeren, **verwijst de Autoriteit naar haar bovenstaande opmerkingen over de uitbreiding van de identificatieplicht en de invoering van indirecte identificatiemethoden**.

109. Wat de regeling voor toegang tot deze informatie betreft (motivering van het verzoek en geen voorafgaande controle), merkt de Autoriteit op dat deze **in overeenstemming is met de vereisten die het Grondwettelijk Hof heeft vastgesteld in zijn arrest nr. 158/2021**. **De Autoriteit neemt hiervan nota.**.

110. Het **nieuwe artikel 25/1, § 2** van de wet BIPT heeft tot doel een officier van gerechtelijke politie van het BIPT toe te staan om, in beginsel na machtiging door een onderzoeksrechter, van een operator te eisen dat hij hem de **metadata van elektronische communicatie** verstrekt die noodzakelijk zijn voor het **onderzoek, de vaststelling of de vervolging van een inbreuk** bedoeld in artikel 145, § 3 of § 3bis van de telecomwet of in artikel 24, § 2 van de wet BIPT.

111. De Autoriteit merkt op dat **niet wordt gespecificeerd tot welke metagegevens** van de elektronische communicatie **de officier van gerechtelijke politie van het BIPT toegang kan hebben**. De ontwerpbepaling is zeer ruim geformuleerd en maakt het mogelijk *a priori* toegang te vragen tot alle door operatoren opgeslagen gegevens, met inbegrip van gegevens die zijn opgeslagen op grond van het nieuwe artikel 126/1 van de telecomwet. Gelet op **de bijzonder ernstige inmenging** als gevolg van de bewaring van gegevens op grond van het nieuwe artikel 126/1 van de telecomwet, vereist het evenredigheidsbeginsel echter, zoals uitgelegd door het HvJEU, dat toegang tot dergelijke gegevens alleen mag worden verleend met het oog op de bestrijding van ernstige criminaliteit. **De Autoriteit stelt vast dat de auteur van het amendement niet motiveert waarom de door de officieren van gerechtelijke politie van het BIPT onderzochte en vervolgde strafbare inbreuken (waarvoor zij toegang tot communicatiemetadata kunnen vragen) onder zware criminaliteit vallen**.

112. **Bij gebrek aan een gemotiveerde rechtvaardiging van het belang van het nagestreefde doel (in het licht van de door het HvJEU benadrukte vereisten), zal de ontwerpbepaling moeten worden gewijzigd om de mogelijkheid uit te sluiten dat het BIPT toegang vraagt tot de gegevens die worden bewaard ter uitvoering van artikel 126/1 van de telecomwet**.

113. Voor het overige merkt de Autoriteit op dat **de modaltiteiten voor toegang tot dergelijke gegevens** (motiveringsvereiste en voorafgaande controle) **voldoen aan de vereisten als opgelegd door het HvJEU** .

114. Het **nieuwe artikel 25/1, § 3** van de wet betreffende het BIPT heeft tot doel de officier van gerechtelijke politie van het BIPT toe te staan de **gegevensbanken te raadplegen** die uitvoering geven aan de artikelen 126, 126/1, 126/2 en 127 van de telecomwet, **teneinde toezicht te houden op de naleving van deze bepalingen**, waarvan de overtreding strafrechtelijk wordt bestraft. De Autoriteit **heeft geen opmerkingen** over deze bepaling.

H. Betreffende de amendementen nrs. 16 tot 18

115. **Amendement nr. 16 beoogt de wijziging van artikel 46bis van het WSV om de procureur des Konings in staat te stellen om, met het oog op de identificatie van de abonnee of de gewoonlijkie gebruiker van een elektronische-communicatiedienst, rechtstreeks of door tussenkomst van de door de koning aangewezen politiedienst, de samenwerking te vragen van:**

(1) banken en financiële instellingen op basis van de referentie van een elektronische bankverrichting die hun vooraf door een operator is meegedeeld (identificatie via een indirecte methode)

(2) gesloten centra en woonunits voor buitenlanders (waar de inschrijving van de abonnee op een elektronische- communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaand meegedeeld zijn door een operator (identificatie via een indirecte methode)

(3) andere rechtspersonen die de abonnee zijn van een operator, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaand meegedeeld zijn door een operator (identificatie via een indirecte methode).

116. Artikel 46 bis van het WSV wordt gewijzigd om uitdrukkelijk te voorzien in de bevoegdheid van de procureur des Konings om de abonnee of de gewoonlijke gebruiker van een elektronische-communicatiedienst te identificeren door middel van een indirecte identificatiemethode, overeenkomstig hetgeen is toegestaan door het nieuwe artikel 127 van de telecomwet (dat bij amendement 6 wordt ingevoegd). In dit verband **verwijst de Autoriteit naar haar bovenstaande opmerkingen over de uitbreiding van de identificatieplicht en de invoering van indirecte identificatiemethoden**.

117. **Amendement nr.17 strekt ertoe artikel 11, § 1, van de wet van 24 januari 1977 aan te vullen om het hoofd van de Dienst Inspectie Consumentenproducten (van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu) in staat te stellen de medewerking te vragen van banken en financiële instellingen «*op basis van de referentie van een elektronische banktransactie die voorafgaand meegedeeld is* ».

118. Uit de ontwerpbepaling, zoals die zal worden ingevoegd in fine van artikel 11, § 1, van de wet van 24 januari 1977, **blijkt niet** dat **de referentie van de elektronische bankverrichting door een telecommunicatieoperator** aan het hoofd van de dienst Inspectie der Consumentenproducten moet zijn meegedeeld. Een dergelijke verduidelijking, die de bevoegdheid van de administratie omkadert, is van essentieel belang om zowel de voorspelbaarheid als de evenredigheid van de inmenging in het

recht op bescherming van persoonsgegevens te waarborgen. **Het amendement moet worden gewijzigd om deze verduidelijking op te nemen**. Voor het overige **verwijst de Autoriteit naar haar bovenstaande opmerkingen** over de **uitbreiding van de identificatieplicht** en de **invoering van een indirecte identificatiemethode** op basis van de referentie van een elektronische banktransactie.

119. **Amendement 18 heeft tot doel artikel 81 van de wet van 2 augustus 2002 te wijzigen zodat de auditeur van de FSMA (of de adjunt-auditeur bij ontstentenis van de auditeur), met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische-communicatiedienst, de medewerking kan vragen van:**
   (1) banken en financiële instellingen op basis van de referentie van een elektronische bankverrichting die hun vooraf door een operator is meegedeeld (identificatie via een indirecte methode)
   (2) gesloten centra en woonunits voor buitenlanders (waar de inschrijving van de abonnee op een elektronische- communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaand meegedeeld zijn door een operator (identificatie via een indirecte methode)
   (3) andere rechtspersonen die de abonnee zijn van een operator, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaand meegedeeld zijn door een operator (identificatie via een indirecte methode).

120. In dit verband **verwijst de Autoriteit naar haar bovenstaande opmerkingen over de uitbreiding van de identificatieplicht en de invoering van indirecte identificatiemethoden**.

OM DIE REDENEN,

De Autoriteit vestigt de aandacht van de regering en de parlementsleden op het volgende :

- Het het ontwerp van herstelwet dataretentie moet grondig worden herzien om tegemoet te komen aan de fundamentele opmerkingen en kanttekeningen van de Autoriteit in haar advies nr. 108/2021. De wetgever moet er in het bijzonder voor zorgen dat het wetsontwerp *de jure of de facto* geen verplichtingen oplegt om verkeers- of locatiegegevens te bewaren van alle of een te groot deel van de gebruikers van elektronische communicatie in België, tenzij er voldoende concrete omstandigheden

zijn waardoor de Staat geacht kan worden te worden geconfronteerd met een ernstige bedreiging van de nationale veiligheid die reëel en actueel is of die te voorzien is (overw.20; overw. 32).)

- De nieuwe definities van "operator" en "elektronische communicatiedienst", in het bijzonder gekoppeld aan de identificatieplicht die wordt opgelegd door de nieuwe artikelen 126 en 127 van de telecomwet maken het onmogelijk - of op zijn minst zeer moeilijk - om anoniem te corresponderen op het internet. Dit is een paradigmaverschuiving ten opzichte van het paradigma van, en de privacyregels die zijn opgelegd door, de e-privacyrichtlijn. Er is een grondig parlementair debat nodig over de gevolgen van deze wijziging, met name wat betreft het recht op privacy en het recht op vrijheid van meningsuiting (overw. 23-24; 40-41).).

- De identificatie van de abonnee van een elektronische-communicatiedienst identificeert niet noodzakelijkerwijs de werkelijke gebruiker van die dienst (overw. 42; 73). Gelet op deze vaststelling en op de moeilijkheid om een negatief bewijs te leveren, verzoekt de Autoriteit de parlementsleden zeer voorzichtig te zijn met het handhaven en uitbreiden van de toepassingsvoorwaarden van een weerlegbaar vermoeden volgens hetwelk «d*e geïdentificeerde persoon wordt vermoed zelf de elektronische-communicatiedienst te gebruiken*» (overw. 78).)

- Wanneer de Koning specifieke, eventueel onrechtstreekse, identificatiemethodes toelaat voor personen die niet over één van de identiteitsdocumenten beschikken opgesomd in het nieuwe artikel 127 van de telecomwet, moet de Koning erop toezien dat de beginselen van noodzakelijkheid en evenredigheid worden nageleefd (overw. 67)

- Met de amendementen wordt beoogd de categorieën van autoriteiten die abonnees en eindgebruikers van elektronische-communicatiediensten kunnen identificeren, uit te breiden, ook via indirecte identificatiemethoden. De parlementsleden moeten zich ervan vergewissen dat deze uitbreiding (en de toegenomen inmenging die zij veroorzaakt in de rechten en vrijheden van de betrokken personen) noodzakelijk is en in verhouding staat tot het nagestreefde doel, aangezien de rechtvaardiging van de noodzaak en de evenredigheid gebaseerd moet zijn op feitelijke en concrete elementen (overw. 74, 108; 116, 120)

- Het is aan de wetgever om zich ervan te vergewissen dat het BIPT wel degelijk toegang moet hebben tot de gegevens waarmee de abonnee of de gewoonlijke gebruiker van de dienst kan worden geïdentificeerd en tot de onbewerkte metagegevens betreffende de communicatie, door met name na te gaan of het BIPT zijn taken niet kan uitvoeren indien het geen toegang heeft tot de communicatiemetagegevens. De Autoriteit benadrukt met name dat, indien het mogelijk is dat het BIPT alle of sommige van de hierboven genoemde taken uitvoert met behulp van geanonimiseerde of gepseudonimiseerde gegevens, het ontwerp moet bepalen dat alleen geanonimiseerde of

gepseudonimiseerde gegevens aan hen mogen worden doorgegeven (overw. 92). Indien en voor zover het BIPT een opdracht van openbaar belang heeft om cyberaanvallen in realtime op te sporen en te stoppen (wat kan inhouden dat bepaalde diensten of IP-adressen moeten worden geblokkeerd om bijvoorbeeld DDOS-aanvallen te stoppen, botnets uit te schakelen of phishing-pogingen te stoppen), begrijpt de Autoriteit dat het BIPT toegang moet kunnen krijgen tot onbewerkte metadata van elektronische communicatie. Gezien de ernst van de inmenging die een dergelijke toegang in het recht op privacy veroorzaakt, acht de Autoriteit het echter van essentieel belang dat er een diepgaand parlementair debat wordt gehouden om de exacte contouren te bepalen van de bevoegdheden en taken van de politie, de gerechtelijke diensten, de inlichtingendiensten, de militaire diensten of de bestuurlijke autoriteiten die verantwoordelijk zijn voor het opsporen en bestrijden van cyberaanvallen (overw. 93)

- Met betrekking tot de nieuwe toestemmingsbevoegdheid die de wijzigingen aan de Autoriteit willen verlenen, verwijst de Autoriteit naar en dringt zij erop aan dat naar behoren rekening wordt gehouden met de opmerkingen in de overwegingen 66 tot en met 73 van advies nr. 32/2022 en de overwegingen 59 tot en met 64 van de bijlage bij het advies over het wetsontwerp tot wijziging van de wet tot oprichting van de GBA (overw. 100-102)

De Autoriteit meent dat de amenemenden als volgt moeten worden aangepast:

- Het nieuwe artikel 126/2, § 1, 9° en 10° schrappen (of althans die waarvoor de auteur de bewaring niet kan rechtvaardigen), tenzij de auteur van het amendement met feitelijke en concrete elementen kan aantonen waarom de bewaring van deze categorieën van gegevens noodzakelijk en evenredig is ten opzichte van het nagestreefde doel, en deze uitleg wordt toegevoegd in de verantwoording van het amendement (overw. 35)

- Het nieuwe artikel 126/2 § 1, 11° schrappen (overw. 36)

- De verkooppunten van elektronische-communicatiediensten verplichten de identificatiegegevens van de abonnees rechtstreeks in de computersystemen van de operator in te voeren en hen verbieden kopieën van identiteitsdocumenten te maken (overw. 46).

- De operatoren en verkoopskanalen van elektronische-communicatiediensten de mogelijkheid ontnemen om een automatische methode te gebruiken voor de vergelijking van de biometrische parameters op de foto van het identiteitsbewijs van de abonnee met die van zijn gezicht (overw. 49-53)

- In het nieuwe artikel 127 § 4, laatste lid van de telecomwet, de woorden «*en de operator de in het derde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast*» en het woord «*kan*» vervangen door het woord «*moet*»(overw. 55)

- Het nieuwe artikel 127, § 5, 3de lid, schrappen en enkel voorzien in de vermelding in de databank die door de operatoren is opgericht krachtens artikel 127 van de telecomwet, van de identiteitsgegevens die worden verzameld bij de raadpleging van de identiteitsdocumenten (overw .57) en, om dezelfde redenen, in het nieuwe artikel 127, § 10, 2de lid, de verplichting schrappen om «*de operator een kopie van het identiteitsdocument van de abonnee te verstrekken, behalve wanneer het gaat om de Belgische elektronische identiteitskaart, overeenkomstig §5, 3de lid*» (overw.82)

- Schrappen van het nieuwe artikel 127 § 5, 4de en 5de lid overw. 58-66)

- Een unieke lijst opstellen van de identificatiegegevens die moeten worden bewaard, zelfs als dat betekent dat bepaalde gegevens alleen moeten worden bewaard voor zover zij voor de betrokkene bestaan (overw.68-69)

- «*de foto van de abonnee, maar enkel voor andere identiteitsstukken dan de Belgische elektronische identiteitskaart*» verwijderen van de maximale lijst van gegevens die mogen/moeten worden bewaard (overw. 70,a))

- Huisadres, e-mailadres en telefoonnummer schrappen van de lijst van identificatiegegevens die operatoren moeten bijhouden (overw. 70 b))

- het "*openbaar veiligheidsnumm**er***" definieren, eventueel door te verwijzen naar regelgefing waarin dit begrip al werd gedefinieerd (overw. 70 c))

- Verduidelijken dat het nummer van het identiteitsdocument alleen kan worden behouden in de situatie waarin de operator nog niet over het Rijksregisternummer beschikt (cons. 70 d))

- Bepalen dat wanneer de abonnee wordt geïdentificeerd aan de hand van een Belgische elektronische identiteitskaart, de operator alleen het rijksregisternummer, de achternaam en de voornaam mag bewaren (overw. 70 e))

- de delegatie aan de Koning ,als bepaald in het nieuwe artikel 127 §6, 2de lid, schrappen (overw. 70 f))

- de geboortedatum en -plaats schrappen van de lijst van gegevens die moeten worden verzameld in het kader van de indirecte identificatiemethode in geval van online elektronische betaling die specifiek is voor het abonnement op een elektronische-communicatiedienst (cons. 76)

- de bewaring van IP-adressen die zijn gebruikt om de account aan te maken en IP-adressen die zijn toegewezen aan de bron van de verbinding, beperken tot 12 maanden na het einde van de sessie (cons. 77)

- Het nieuwe artikel 127, § 10, vijfde lid, schrappen, tenzij de regering met feitelijke en concrete bewijzen kan aantonen dat het wel degelijk noodzakelijk en evenredig is om het chassisnummer van het voertuig waarin een van de SIM-kaarten of een gelijkwaardige kaart is ingebouwd, alsook het verband tussen het chassisnummer en het nummer van deze kaart te bewaren (in dat geval moet de rechtvaardiging worden gevonden in de motivering van het amendementsvoorstel) (overw. 86)

- het verbod dat het nieuwe artikel 127/4 van de telecomwet oplegt, schrappen (overw. 88)

- uitsluiting van de mogelijkheid voor het BIPT om toegang te vragen tot de gegevens die worden bewaard ter uitvoering van artikel 126/1 van de telecomwet (overw. 9-98; 11-112)

- voor elke opdracht van het BIPT de categorieën van gegevens identificeren waartoe deze instelling toegang moet hebben om de haar toevertrouwde opdrachten van openbare dienst te kunnen vervullen (overw. 99)

- de modaliteiten van de voorafgaande controle van de toegang tot metagegevens door het BIPT herzien overeenkomstig de opmerkingen in de overwegingen 66 tot en met 73 van advies nr. 33/2022 van de Autoriteit (overw. 100-102)

- In het dispositief van artikel 11 § 1 van de wet van 24 januari 1977 te preciseren dat de referentie van de elektronische bankverrichting door een telecomoperator aan het hoofd van de Dienst Inspectie der Consumentenproducten moet zijn meegedeeld (overw. 118)

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