HOOFDSTUK 5. — *Inwerkingtreding*

Art. 5. Deze wet treedt in werking de dag waarop deze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te L'Île d'Yeu, 30 juli 2022.

FILIP

Van Koningswege :

De Minister van Volksgezondheid,
F. VANDENBROUCKE

Met 's Lands zegel gezegeld:

De Minister van Justitie,

V. VAN QUICKENBORNE

Nota

(1) Stukken van de Kamer van Volksvertegenwoordigers:
55-2801/2021/2022
Nr. 1 : Wetsontwerp.
Nr. 2 : Amendement.
Nr. 3 : Verslag.
Nr. 4 : Artikelen bij eerste stemming aangenomen.
Nr. 5 : Amendement.
Nr. 6 : Verslag.
Nr. 7 : Aangenomen tekst.
Nr. 8 : Amendement.
Nr. 9 : Aangenomen tekst.

CHAPITRE 5. — *Entrée en vigueur*

Art. 5. La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'Etat et publiée par le *Moniteur belge.*

Donné à L'Île d'Yeu, le 30 juillet 2022.

PHILIPPE

Par le Roi :

Le Ministre de la Santé publique,
F. VANDENBROUCKE

Scellé du sceau de l'Etat :

Le Ministre de la Justice,

V. VAN QUICKENBORNE

Note

(1) Documents de la Chambre des représentants
55-2801/2021/2022
N° 1 : Projet de loi.
N° 2 : Amendement.
N° 3 : Rapport.
N° 4 : Articles adoptés au 1er vote.
N° 5 : Amendement.
N° 6 : Rapport.
N° 7 : Texte adopté.
N° 8 : Amendement.
N° 9 : Texte adopté.

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2022/15454]

20 JULI 2022. — Wet 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 (1)

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK 1. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2. — *Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie*

Art. 2. In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 17 februari 2022, worden de volgende wijzigingen aangebracht:

1° de bepalingen onder 5/5° en 5/6° worden ingevoegd, luidende:

"5/5° "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst;

5/6° "kwaadwillig gebruik van het netwerk of van de dienst": gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen;";

2° in de plaats van de bepaling onder 74°, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een bepaling onder 74° ingevoegd, luidende:

"74° "oproeppoging zonder resultaat": iedere communicatie waarbij een oproep wel werd doorgezonden, maar onbeantwoord is gebleven of door de netwerkbeheerder is beantwoord;";

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2022/15454]

20 JUILLET 2022. — Loi relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (1)

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

CHAPITRE 1er. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2. — *Modifications de la loi du 13 juin 2005 relative aux communications électroniques*

Art. 2. À l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, modifié en dernier lieu par la loi du 17 février 2022, les modifications suivantes sont apportées:

1° les 5/5° et 5/6° sont insérés, rédigés comme suit:

"5/5° "une fraude": un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques;

5/6° "utilisation malveillante du réseau ou du service": utilisation du réseau ou du service de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages;";

2° à la place du 74°, annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un 74° rédigé comme suit:

"74° "appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau;";

3° het artikel wordt aangevuld met de bepalingen onder 91°, 92° en 93°, luidende:

"91° "elektronische-communicatiegegevens": de inhoud en de metagegevens van elektronische communicatie;

92° "inhoud van elektronische communicatie": de inhoud die wordt uitgewisseld door middel van elektronische-communicatiediensten, met name tekst, spraak, video, beelden en geluid;

93° "elektronische-communicatiemetagegevens": de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.".

Art. 3. Artikel 107/5 van dezelfde wet, ingevoegd bij de wet van 21 december 2021, wordt vervangen als volgt:

"Art. 107/5. § 1. Ter bevordering van de digitale veiligheid is het gebruik van versleuteling vrij binnen de in de paragrafen 2 tot 4 gestelde grenzen.

§ 2. Het gebruik van versleuteling mag noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of het verstrekken van de identificatiegegevens van de oproeper, niet verhinderen.

§ 3. Het gebruik van versleuteling door een operator, met als doel de veiligheid van de communicatie te waarborgen, mag geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie.

§ 4. Het gebruik van versleuteling door een buitenlandse operator, wiens eindgebruiker of abonnee zich op het Belgisch grondgebied bevindt, mag de uitvoering van een verzoek van een bevoegde overheid, zoals bedoeld in de paragrafen 2 en 3, niet verhinderen.

Elk contractueel beding dat door de operatoren wordt opgesteld en de uitvoering van het eerste lid belemmert, is verboden en van rechtswege nietig.".

Art. 4. In titel IV, hoofdstuk III, afdeling 1, onderafdeling 7, van dezelfde wet wordt een artikel 121/8 ingevoegd, luidende:

"Art. 121/8. § 1. Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden.

De Koning kan de door de operatoren krachtens het eerste lid te treffen maatregelen preciseren.

Het Instituut is bevoegd om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen, met het oog op de toepassing van deze paragraaf.

§ 2. Wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden, die per geval onderzocht moeten worden, kunnen de in paragraaf 1, eerste lid, bedoelde gepaste maatregelen met name het volgende omvatten:

— maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie;

— maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur.".

Art. 5. In artikel 122 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt het tweede lid opgeheven;

2° in paragraaf 2 worden de volgende wijzigingen aangebracht:

a) het eerste lid wordt vervangen als volgt:

"In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken.";

3° l'article est complété par les 91°, 92° et 93°, rédigés comme suit:

"91° "données de communications électroniques": le contenu et les métadonnées de communications électroniques;

92° "contenu de communications électroniques": le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son;

93° "métadonnées de communications électroniques": les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.".

Art. 3. L'article 107/5 de la même loi, inséré par la loi du 21 décembre 2021, est remplacé par ce qui suit:

"Art. 107/5. § 1er. Afin de favoriser la sécurité numérique, l'utilisation de la cryptographie est libre dans les limites prévues aux paragraphes 2 à 4.

§ 2. Le recours à la cryptographie ne peut pas empêcher les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant.

§ 3. Le recours à la cryptographie, utilisée par un opérateur, visant à garantir la sécurité des communications, ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public.

§ 4. L'utilisation de la cryptographie par un opérateur étranger, dont l'utilisateur final ou l'abonné est situé sur le territoire belge, ne peut pas empêcher l'exécution d'une demande d'une autorité compétente telle que visée aux paragraphes 2 et 3.

Toute clause contractuelle prise par les opérateurs faisant obstacle à l'exécution de l'alinéa 1er est interdite et nulle de plein droit.".

Art. 4. Dans le titre IV, chapitre III, section 1re, sous-section 7, de la même loi, il est inséré un article 121/8, rédigé comme suit:

"Art. 121/8. § 1er. Sans prendre connaissance du contenu des communications, les opérateurs prennent les mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés.

Le Roi peut préciser les mesures à prendre par les opérateurs en vertu de l'alinéa 1er.

L'Institut a le pouvoir de donner des instructions contraignantes, y compris des instructions concernant les délais d'exécution, en vue de l'application du présent paragraphe.

§ 2. Lorsque cela se justifie au regard de la gravité des circonstances, qui doivent être examinées au cas par cas, les mesures appropriées visées au paragraphe 1er, alinéa 1er, peuvent comprendre notamment:

— des mesures au niveau du réseau, tels que le blocage des numéros, de services, des URLs, de noms de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique;

— des mesures au niveau de l'utilisateur final, telles que la désactivation complète ou partielle de certains services ou équipements.".

Art. 5. À l'article 122 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, l'alinéa 2 est abrogé;

2° dans le paragraphe 2, les modifications suivantes sont apportées:

a) l'alinéa 1er est remplacé par ce qui suit:

"Par dérogation au paragraphe 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin.";

b) in het tweede lid worden de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

c) in het derde lid wordt het woord "opgesomd" vervangen door het woord "bedoeld";

3° in paragraaf 3 worden de volgende wijzigingen aangebracht:

a) in het eerste lid, 2°, worden de woorden "de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat verkeersgegevens die op hem betrekking hebben worden verwerkt" vervangen door de woorden "de toestemming in de zin van artikel 4, 11), van de AVG";

b) in het eerste lid, 3°, worden de woorden "op eenvoudige wijze" vervangen door de woorden "makkelijk en te allen tijde";

c) in het tweede lid worden de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

4° paragraaf 4 wordt vervangen als volgt:

"§ 4. In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, en voor zover hij deze verwerkt of genereert in het kader van de verstrekking van dat netwerk of van die dienst:

1° bewaart de operator, in het kader van de verstrekking van een interpersoonlijke communicatiedienst en gedurende vier maanden vanaf de datum van de communicatie, de daartoe noodzakelijke verkeersgegevens onder de volgende verkeersgegevens:

— de identifier van de bron van de communicatie;

— de identifier van de bestemming van de communicatie;

— de precieze datums en tijdstippen van het begin en het einde van de communicatie;

— de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie;

2° bewaart de operator gedurende twaalf maanden vanaf de datum van de communicatie de volgende verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten, teneinde de persoon die de communicatie doet, te identificeren:

— het telefoonnummer aan de bron van de binnenkomende communicatie, of;

— het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort, en;

— de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie;

3° bewaart de operator de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van vier maanden bedoeld in 1°;

4° bewaart de operator de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in 2°;

5° verwerkt de operator de noodzakelijke verkeersgegevens voor deze doeleinden, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, preciseren en uitbreiden.

b) dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

c) dans l'alinéa 3, le mot "énumérées" est remplacé par le mot "visées";

3° dans le paragraphe 3, les modifications suivantes sont apportées:

a) dans l'alinéa 1er, 2°, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées" sont remplacés par les mots "le consentement au sens de l'article 4, 11), du RGPD";

b) dans l'alinéa 1er, 3°, les mots "de manière simple" sont remplacés par les mots "facilement et à tout moment";

c) dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

4° le paragraphe 4 est remplacé par ce qui suit:

"§ 4. Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, et pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ce réseau ou de ce service, l'opérateur:

1° conserve, dans le cadre de la fourniture d'un service de communications interpersonnelles et pendant quatre mois à partir de la date de la communication, les données de trafic nécessaires à ces fins parmi les données de trafic suivantes:

— l'identifiant de l'origine de la communication;

— l'identifiant de la destination de la communication;

— les dates et heures précises de début et de fin de la communication;

— la localisation des équipements terminaux des parties à la communication au début et à la fin de la communication;

2° conserve pendant douze mois à partir de la date de la communication les données de trafic suivantes relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles afin d'identifier l'auteur de la communication:

— le numéro de téléphone à l'origine de la communication entrante, ou;

— l'adresse IP ayant servi à l'envoi de la communication entrante, l'horodatage et le port utilisé, et;

— les dates et heures précises du début et de fin de la communication entrante;

3° conserve les données visées au 1° qui sont relatives à une fraude spécifique identifiée ou une utilisation malveillante du réseau spécifique identifiée le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de quatre mois visé au 1°;

4° conserve les données de trafic visées au 2° et relatives à une utilisation malveillante spécifique du réseau, le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de douze mois visé au 2°;

5° traite les données de trafic nécessaires à ces fins, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.

Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins.

Le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe.

In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen.";

5° een paragraaf 4/1 wordt ingevoegd, luidende:

"§ 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

De operatoren mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.

De operatoren mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in het tweede lid.

In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen.";

6° een paragraaf 4/2 wordt ingevoegd, luidende:

"§ 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur.";

7° paragraaf 5 wordt vervangen als volgt:

"§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel bedoeld in artikel 127/3.";

8° in paragraaf 6 worden de woorden "Het Instituut" vervangen door de woorden "Het Instituut, de Ombudsdienst voor telecommunicatie,".

Art. 6. In artikel 123 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen:

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal twaalf maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal vier maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

3° wanneer de gegevens anoniem gemaakt zijn;

4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm.";

2° in paragraaf 2 worden in de bepaling onder 2°, de woorden "de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke, vertegenwoordiger aanvaardt dat locatiegegevens die op hem betrekking hebben worden verwerkt" vervangen door de woorden "de toestemming in de zin van artikel 4, 11), van de AVG";

En cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée.";

5° il est inséré un paragraphe 4/1 rédigé comme suit:

"§ 4/1. Par dérogation au paragraphe 1er, les opérateurs peuvent conserver et traiter les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

Les opérateurs peuvent les conserver pour une durée de douze mois à partir de la date de la communication.

Les opérateurs peuvent conserver les données visées à l'alinéa 1er relatives à une atteinte spécifique à la sécurité du réseau pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de douze mois visé à l'alinéa 2.

En cas d'atteinte à la sécurité de leurs réseaux et services de communications électroniques, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec l'atteinte à la sécurité de leurs réseaux et services de communications électroniques.";

6° il est inséré un paragraphe 4/2 rédigé comme suit:

"§ 4/2. Par dérogation au paragraphe 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation imposée par une norme législative formelle, pour la durée requise à cette fin.";

7° le paragraphe 5 est remplacé par ce qui suit:

"§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination visée à l'article 127/3.";

8° dans le paragraphe 6, les mots "L'Institut" sont remplacés par les mots "L'Institut, le Service de médiation pour les télécommunications,".

Art. 6. À l'article 123 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021, les modifications suivantes sont apportées:

1° le paragraphe 1er est remplacé par ce qui suit:

"§ 1er. Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants:

1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées maximum douze mois à partir de la date de la communication, sauf en cas d'atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées maximum quatre mois à partir de la date de la communication, sauf en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

3° lorsque les données ont été rendues anonymes;

4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service qui fait usage de données de trafic ou de localisation;

5° lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle.";

2° dans le paragraphe 2, dans le 2°, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées" sont remplacés par les mots "le consentement au sens de l'article 4, 11), du RGPD";

3° in paragraaf 4 wordt het eerste lid vervangen als volgt:

"De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator bedoeld in artikel 127/3.".

Art. 7. Artikel 125, § 2, van dezelfde wet, opgeheven bij artikel 3 van de wet van 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt opgeheven.

Art. 8. Artikel 126 van dezelfde wet, vervangen bij artikel 5 van de wet van 30 juli 2013, zelf vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, en bij artikel 4 van de wet van 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt vervangen als volgt:

"Art. 126. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten:

1° het Rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is;

2° de eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst;

3° de contactgegevens van de abonnee die verstrekt zijn bij de inschrijving op de dienst, met name zijn telefoonnummer, zijn e-mailadres en zijn postadres;

4° de datum en het tijdstip van inschrijving op de dienst en van de activering van de dienst en de elementen aan de hand waarvan de plaats kan bepaald worden waarvandaan die inschrijving en die activering zijn uitgevoerd, met name:

— het fysieke adres van het verkooppunt waar de inschrijving of activering heeft plaatsgevonden, of;

— het fysieke adres van het netwerkaansluitpunt dat gediend heeft voor de inschrijving of de activering, of;

— het IP-adres dat gediend heeft voor de inschrijving of de activering, alsook de bronpoort van de verbinding en het tijdstempel, of;

— in het kader van een mobiel telefoonnetwerk, de geografische locatie van de eindapparatuur die de inschrijving of de activering aan de hand van een telefoonnummer mogelijk heeft gemaakt;

5° het fysieke leveringsadres van de dienst;

6° het facturatieadres van de dienst en de gegevens betreffende de betalingswijze en het betaalmiddel, het tijdstip van de betalingen en de referentie van de betalingstransactie in geval van onlinebetaling;

7° de hoofddienst en de aanvullende diensten die de abonnee kan gebruiken;

8° de datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van die diensten en de datum van beëindiging van die diensten;

9° in geval van overdracht van de identifier van de abonnee, zoals zijn telefoonnummer, de identiteit van de operator die de identifier overdraagt en de identiteit van de operator naar wie de identifier wordt overgedragen en de datum waarop de overdracht wordt uitgevoerd;

10° het toegewezen telefoonnummer;

11° het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden;

12° de internationale identiteit van de mobiele abonnee, "*International Mobile Subscriber Identity*", afgekort "IMSI";

13° de permanente identifier van het abonnement, "*Subscription Permanent Identifier*", afgekort "SUPI";

14° de verdoken identifier van het abonnement, "*Subscription Concealed Identifier*", afgekort "SUCI";

15° het IP-adres aan de bron van de verbinding, het tijdstempel van de toewijzing alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de poorten die daaraan zijn toegewezen;

3° dans le paragraphe 4, l'alinéa 1er est remplacé par ce qui suit:

"Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit le service qui fait usage de données de trafic ou de localisation, ou par la Cellule de coordination de l'opérateur visée à l'article 127/3.".

Art. 7. L'article 125, § 2, de la même loi, abrogé par l'article 3 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, est abrogé.

Art. 8. L'article 126 de la même loi, remplacé par l'article 5 de la loi du 30 juillet 2013, annulé lui-même par l'arrêt n° 84/2015 de la Cour constitutionnelle, et par l'article 4 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, est remplacé par ce qui suit:

"Art. 126. § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents qui permettent la fourniture de ces services, conservent les données suivantes, pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services:

1° le numéro de Registre national ou un numéro équivalent, le nom et le prénom de l'utilisateur final qui est une personne physique ou la dénomination de l'abonné qui est une personne morale;

2° l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service;

3° les coordonnées de l'abonné qui ont été fournies lors de la souscription au service, notamment son numéro de téléphone, son adresse e-mail et son adresse postale;

4° la date et l'heure de la souscription au service et de l'activation du service et les éléments permettant de déterminer le lieu à partir duquel cette souscription et cette activation ont été effectuées, à savoir notamment:

— l'adresse physique du point de vente où la souscription ou l'activation ont eu lieu, ou;

— l'adresse physique du point de terminaison du réseau ayant servi à la souscription ou à l'activation, ou;

— l'adresse IP ayant servi à la souscription ou à l'activation ainsi que le port source de la connexion et l'horodatage, ou;

— dans le cadre d'un réseau téléphonique mobile, la localisation géographique de l'équipement terminal qui a permis la souscription ou l'activation au moyen d'un numéro de téléphone;

5° l'adresse physique de livraison du service;

6° l'adresse de facturation du service et les données relatives au type et au moyen de paiement, à la date des paiements, et la référence de l'opération de paiement en cas de paiement en ligne;

7° le service principal et les services annexes que l'abonné peut utiliser;

8° la date à partir de laquelle ces services peuvent être utilisés, la date de la première utilisation de ces services et la date de fin de ces services;

9° en cas de transfert de l'identifiant de l'abonné, tel son numéro de téléphone, l'identité de l'opérateur qui transfère l'identifiant et l'identité de l'opérateur auquel l'identifiant est transféré et la date à laquelle le transfert est effectué;

10° le numéro de téléphone attribué;

11° l'adresse de messagerie principale et les adresses de messagerie employées comme alias;

12° l'identité internationale d'abonné mobile, "International Mobile Subscriber Identity", en abrégé "IMSI";

13° l'identifiant permanent d'abonnement, "Subscription Permanent Identifier", en abrégé "SUPI";

14° l'identifiant caché d'abonnement, "Subscription Concealed Identifier", en abrégé "SUCI";

15° l'adresse IP à la source de la connexion, l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, les ports qui lui ont été attribués;

16° de identifier van de eindapparatuur van de eindgebruiker, of indien de operator dit niet verwerkt of genereert, de identifier van de apparatuur die zich het dichtste bij die eindapparatuur bevindt, met name:

— de internationale identiteit van de mobiele apparatuur, "*International Mobile Equipment Identity*", afgekort "IMEI";

— de permanente identifier van de apparatuur, "*Permanent Equipment Identifier*", afgekort "PEI";

— het adres van de controller van de toegang tot het netwerk, "*Media Access Control address*", afgekort "MAC";

17° de andere identifiers met betrekking tot de eindgebruiker, tot de eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren hoeven de MAC-adressen bedoeld in het eerste lid, 16°, derde streepje, niet te bewaren voor de elektronische-communicatiediensten die ze enkel aan ondernemingen of rechtspersonen aanbieden.

Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatiemetagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur.

De Koning:

1° kan de gegevens bedoeld in het eerste lid preciseren;

2° bepaalt de vereisten inzake nauwkeurigheid en betrouwbaarheid waaraan deze gegevens moeten beantwoorden.

§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, 1° tot 14°, bedoelde gegevens tot zolang de elektronische-communicatiedienst gebruikt wordt en tot twaalf maanden na het einde van de dienst.

De operatoren bewaren de in paragraaf 1, eerste lid, 15° en 16°, bedoelde gegevens gedurende een periode van twaalf maanden na het einde van de sessie.

In afwijking van het tweede lid wordt de bewaringstermijn van de in paragraaf 1, eerste lid, 16°, derde streepje, bedoelde gegevens, teruggebracht tot zes maanden na het einde van de sessie indien de operator een ander gegeven zoals bedoeld in paragraaf 1, eerste lid, 16°, bewaart.

De operatoren bewaren de gegevens bedoeld in paragraaf 1, eerste lid, 17°, gedurende de door de Koning bepaalde periode. Die periode mag niet langer zijn dan de in het eerste lid bedoelde bewaringstermijn.

Het koninklijk besluit bedoeld in paragraaf 1, eerste lid, 17°, en vierde lid, en in paragraaf 2, vierde lid, wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad.".

Art. 9. In dezelfde wet wordt in de plaats van artikel 126/1, ingevoegd bij artikel 5 van de wet van 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, het als volgt luidende artikel 126/1 ingevoegd:

"Art. 126/1. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die onderliggende en elektronische-communicatienetwerken aanbieden, de in artikel 126/2, § 2, bedoelde gegevens voor de geografische zones bedoeld in artikel 126/3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in artikel 126/3.

Elke operator bewaart de gegevens die door hem gegenereerd of verwerkt zijn in het kader van de verstrekking van de betrokken van de verstrekking van de betrokken elektronische-communicatiediensten en -netwerken.

Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

§ 2. 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, § 2.

§ 3. De operatoren bewaren de verkeersgegevens voor iedere communicatie of alle oproeppogingen zonder resultaat die vanuit of naar een geografisch gebied als bedoeld in artikel 126/3 worden gevoerd.

16° l'identifiant de l'équipement terminal de l'utilisateur final, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment:

— l'identité internationale d'équipement mobile, "International Mobile Equipment Identity", en abrégé "IMEI";

— l'identifiant permanent de l'équipement, "Permanent Equipment Identifier", en abrégé "PEI";

— l'adresse du contrôleur d'accès au réseau, "Media Access Control address", en abrégé "MAC";

17° les autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs ne doivent pas conserver les adresses MAC visées à l'alinéa 1er, 16°, troisième tiret, pour les services de communications électroniques qu'ils offrent uniquement à des entreprises ou à des personnes morales.

L'arrêté royal visé à l'alinéa 1er, 17°, ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication, ou sur la localisation de l'équipement terminal.

Le Roi:

1° peut préciser les données visées à l'alinéa 1er;

2° fixe les exigences en matière de précision et de fiabilité auxquelles ces données doivent répondre.

§ 2. Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 1° à 14°, aussi longtemps que le service de communications électroniques est utilisé ainsi que douze mois après la fin du service.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 15° et 16°, pour une durée de douze mois après la fin de la session.

Par dérogation à l'alinéa 2, la durée de conservation des données visées au paragraphe 1er, alinéa 1er, 16°, troisième tiret, est réduite à six mois après la fin de la session lorsque l'opérateur conserve une autre donnée visée au paragraphe 1er, alinéa 1er, 16°.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 17°, pour la durée fixée par le Roi. Cette durée ne peut pas être plus longue que la durée de conservation visée à l'alinéa 1er.

L'arrêté royal visé au paragraphe 1er, alinéa 1er, 17°, et alinéa 4 et au paragraphe 2, alinéa 4, est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres.".

Art. 9. Dans la même loi, à la place de l'article 126/1, inséré par l'article 5 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un article 126/1 rédigé comme suit:

"Art. 126/1. § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées à l'article 126/2, § 2, pour les zones géographiques visées à l'article 126/3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans l'article 126/3.

Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communications électroniques concernés.

Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.

§ 2. Les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er, sont énumérées à l'article 126/2, § 2.

§ 3. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée à l'article 126/3 ou vers une telle zone.

Indien de operator, als gevolg van de door hem gebruikte technologie, niet in staat is de eindapparatuur die betrokken is bij de communicatie, met inbegrip van de oproeppoging zonder resultaat, nauwkeuriger te lokaliseren dan de lokalisatie ervan op het nationale grondgebied, bewaart de operator de in artikel 126/2, § 2, bedoelde gegevens gedurende de kortste overeenkomstig dit artikel en artikel 126/3 bepaalde termijn, op voorwaarde dat overeenkomstig dit artikel en artikel 126/3 het gehele nationale grondgebied gedekt is door een bewaarplicht. Indien niet aan deze voorwaarde is voldaan, bewaart de operator op wie dit lid van toepassing is deze gegevens niet.

Wanneer de eindgebruiker zich tijdens een elektronische communicatie verplaatst, bewaart de operator de verkeersgegevens voor zover de eindgebruiker zich op een bepaald moment van de communicatie bevindt in een zone bedoeld in artikel 126/3.

De operatoren bewaren de gegevens met betrekking tot de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, die opgesomd zijn in artikel 126/2, § 2, wanneer die apparatuur zich bevindt in een in artikel 126/3 bedoelde zone.

Om te bepalen of eindapparatuur zich in een geografische zone als bedoeld in artikel 126/3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens als mogelijk is. Zij maken hiervoor, indien beschikbaar, gebruik van de satellietlocatie van eindapparatuur.

Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een in artikel 126/3 bedoelde zone, bewaart hij 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.

Wanneer een aggregatiepunt van de operator, zoals een antenne, verschillende in artikel 126/3 bedoelde geografische zones dekt die onderworpen zijn aan een verschillende bewaringstermijn, bewaart de operator de gegevens voor dat aggregatiepunt gedurende de kortste bewaringstermijn.

Wanneer op grond van dit artikel en van artikel 126/3 verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, bewaren de operatoren de gegevens gedurende de kortste termijn.

§ 4. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende bepalen:

— de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in artikel 126/3 bedoelde zones;

— de lijst van de verschillende autoriteiten die bevoegd zijn voor de in artikel 126/3, §§ 2 tot 5, bedoelde aangelegenheden;

— de nadere regels voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de nadere regels voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;

— in voorkomend geval, de bijkomende geografische zones bedoeld in artikel 126/3, § 3, m), § 4, g), en § 5, f).

Het koninklijk besluit bedoeld in het eerste lid, vierde streepje, wordt elke drie jaar hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

§ 5. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité Inlichtingen en Veiligheid, van het Instituut en de autoriteiten bevoegd voor de bescherming van de gegevens, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 4 bedoelde koninklijk besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 4 bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in artikel 126/3, §§ 3 tot 5, en of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Lorsque, compte tenu de la technologie utilisée par l'opérateur, celui-ci n'est pas en mesure de localiser l'équipement terminal ayant participé à la communication, y compris l'appel infructueux, de façon plus précise que sa localisation sur le territoire national, l'opérateur conserve les données visées à l'article 126/2, § 2, pour la durée la plus courte fixée en exécution du présent article et de l'article 126/3, à la condition qu'en exécution du présent article et de l'article 126/3 l'ensemble du territoire national soit soumis à une obligation de conservation. Lorsque cette condition n'est pas remplie, l'opérateur concerné par le présent alinéa ne conserve pas ces données.

Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur conserve les données de trafic pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée à l'article 126/3.

Les opérateurs conservent les données relatives à la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, énumérées à l'article 126/2, § 2, lorsque cet équipement se trouve dans une zone visée à l'article 126/3.

Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée à l'article 126/3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent, si disponible à cet effet, la localisation satellitaire d'un équipement terminal.

Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une zone visée à l'article 126/3, il conserve les données nécessaires pour couvrir la totalité de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

Lorsqu'un point d'agrégation de l'opérateur, telle une antenne, couvre plusieurs zones géographiques visées à l'article 126/3 qui sont soumises à des durées de conservation différentes, l'opérateur conserve les données pour ce point d'agrégation pendant la durée de conservation la plus courte.

Lorsqu'en application du présent article et de l'article 126/3, différentes durées de conservation sont applicables aux mêmes données, les opérateurs conservent les données pendant la durée la plus courte.

§ 4. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, et après avis des autorités de protection des données compétentes et de l'Institut, les éléments suivants:

— les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées à l'article 126/3;

— la liste des différentes autorités compétentes dans les matières visées à l'article 126/3, §§ 2 à 5;

— les modalités de communication des informations par les autorités compétentes au service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er;

— s'il échet, les zones géographiques additionnelles visées à l'article 126/3, § 3, m), § 4, g), et § 5, f).

L'arrêté royal visé à l'alinéa 1er, quatrième tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.

§ 5. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 4, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 4 répondent toujours aux critères visés à l'article 126/3, §§ 3 à 5, et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

Het evaluatieverslag bevat ook het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van dit artikel en artikel 126/3 van toepassing is.

Dit evaluatieverslag wordt gestuurd naar het Controleorgaan op de politionele informatie en naar het Vast Comité I.".

Art. 10. In dezelfde wet wordt een artikel 126/2 ingevoegd, luidende:

"Art. 126/2. § 1. Voor de toepassing van dit artikel wordt verstaan onder "communicatie", informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een publiek beschikbare elektronische-communicatiedienst, met uitsluiting van de informatie die via een openbare omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve in de mate waarin de informatie kan worden gelinkt aan de identificeerbare abonnee of gebruiker die deze informatie ontvangt.

§ 2. De gegevens bedoeld in artikel 126/1, § 2, die in uitvoering van de artikelen 126/1 en 126/3 bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook door de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende:

1° de beschrijving en de technische karakteristieken van de elektronische-communicatiedienst die werd aangewend tijdens de communicatie;

2° de identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14°, en 16°, van de geadresseerde van de communicatie;

3° 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;

4° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

5° de datum en het exacte tijdstip van de aanvang en het einde van de sessie van de betrokken elektronische-communicatiedienst, waaronder de datum en het exacte tijdstip van de aanvang en het einde van de oproep;

6° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, 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;

7° het tijdens de duur van de sessie geüploade en gedownloade volume van gegevens;

8° voor wat betreft de mobiele elektronische-communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens 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° 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° de andere identifiers met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

In afwijking van de artikelen 126/1 en 126/3 bedraagt de bewaartermijn van het gegeven bedoeld in het eerste lid, 8°, zes maanden nadat het is gegenereerd of verwerkt.

Het koninklijk besluit bedoeld in het eerste lid, 10°, slaat niet op de inhoud van de elektronische communicatie.

De Koning kan, na advies van de Gegevens-beschermingsautoriteit en het Instituut, de gegevens bedoeld in eerste lid, preciseren.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

Le rapport d'évaluation comprend également le pourcentage du territoire national auquel s'applique l'obligation de conservation des données en vertu du présent article et de l'article 126/3.

Ce rapport d'évaluation est envoyé à l'Organe de contrôle de l'information policière et au Comité permanent R.".

Art. 10. Dans la même loi, il est inséré un article 126/2, rédigé comme suit:

"Art. 126/2. § 1er. Pour l'application du présent article, il y a lieu d'entendre par "communication", toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public, à l'exclusion des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.

§ 2. Les données visées à l'article 126/1, § 2, qui doivent être conservées en exécution des articles 126/1 et 126/3 par les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que par les opérateurs fournissant les réseaux de communications électroniques sous-jacents qui permettent la fourniture de ces services, sont les suivantes:

1° la description et les caractéristiques techniques du service de communications électroniques utilisé lors de la communication;

2° les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14°, et 16°, du destinataire de la communication;

3° pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués;

4° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris celles vers lesquelles l'appel a été transféré;

5° la date et l'heure exacte du début et de la fin de la session du service de communications électroniques concerné, en ce compris la date et l'heure exacte du début et de la fin de l'appel;

6° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisées pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations;

7° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session;

8° pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement terminal au réseau en raison de l'extinction de cet équipement;

9° pour ce qui concerne les services de communications électroniques mobiles, la localisation de l'équipement terminal et la date et l'heure de cette localisation chaque fois que l'opérateur cherche à connaître quels équipements terminaux sont connectés à son réseau;

10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, après avis de l'Autorité de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Par dérogation aux articles 126/1 et 126/3, la durée de conservation de la donnée visée à l'alinéa 1er, 8°, est de six mois après avoir été générée ou traitée.

L'arrêté royal visé à l'alinéa 1er, 10°, ne porte pas sur le contenu des communications électroniques.

Le Roi peut, après avis de l'Autorité de protection des données et de l'Institut, préciser les données visées à l'alinéa 1er.

§ 3. De combinatie van de gegevens bewaard in uitvoering van artikel 126 en van dit artikel moet het mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten inzake nauwkeurigheid en betrouwbaarheid bepalen waaraan de gegevens bedoeld in dit artikel moeten beantwoorden.".

Art. 11. In dezelfde wet wordt een artikel 126/3 ingevoegd, luidende:

"Art. 126/3. § 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:

— de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;

— de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

§ 3. La combinaison des données conservées en exécution de l'article 126 et du présent article doit permettre d'établir la relation entre l'origine de la communication et sa destination.

Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences en matière de précision et de fiabilité auxquelles les données visées au présent article doivent répondre.".

Art. 11. Dans la même loi, il est inséré un article 126/3, rédigé comme suit:

"Art. 126/3. § 1er. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée des:

— arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

— zones de police dans lesquelles au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.

Les statistiques relatives au nombre d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.

Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.

§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.

§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;

b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen en de stadhuizen;

iii) het koninklijk paleis;

iv) de koninklijke domeinen;

v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;

vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:

i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

h) les établissements visés à l'article 3.1.a), de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.

§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:

i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:

i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;

ii) la Banque nationale de Belgique;

g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

Art. 12. Artikel 127 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021, wordt vervangen als volgt:

"Art. 127. § 1. Dit artikel is van toepassing op de operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers.

Het is verboden om in België, inclusief via het internet, zonder het akkoord van de buitenlandse onderneming die de voor het publiek beschikbare elektronische-communicatiedienst verstrekt, het volgende aan te bieden aan de eindgebruikers:

— voorafbetaalde kaarten of abonnementen van die onderneming die hen in staat stellen om er een elektronische-communicatiedienst te gebruiken;

— geconnecteerde voorwerpen waarin een product van die onderneming is geïntegreerd en die hen in staat stellen om er een internettoegangsdienst of een interpersoonlijke communicatiedienst van een operator te gebruiken.

g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.

À l'exception de la liste des lieux visés au paragraphe 4, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au *Moniteur belge*.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

Art. 12. L'article 127 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021, est remplacé par ce qui suit:

"Art. 127. § 1er. Le présent article s'applique aux opérateurs qui fournissent en Belgique, aux utilisateurs finaux, un service de communications électroniques.

Il est interdit de distribuer en Belgique, en ce compris par internet, aux utilisateurs finaux, sans l'accord de l'entreprise étrangère qui fournit le service de communications électroniques accessible au public:

— des cartes prépayées ou des abonnements de cette entreprise qui leur permettent d'y utiliser un service de communications électroniques;

— des objets connectés dans lesquels un produit de cette entreprise est intégré et qui leur permettent d'y utiliser un service d'accès à internet ou un service de communication interpersonnelle d'un opérateur.

De persoon die deze voorafbetaalde kaarten, deze abonnementen of deze geconnecteerde voorwerpen aanbiedt in België, verstrekt aan de officieren van gerechtelijke politie van het Instituut, wanneer zij daarom verzoeken, het bewijs van dat akkoord.

Indien de onderneming akkoord gaat, is zij de operator en schikt zij zich naar artikel 9, § 1.

§ 2. Voor de toepassing van dit artikel wordt verstaan onder:

1° "elektronische-communicatiebetaaldienst": 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;

2° "gratis elektronische-communicatiedienst": de elektronische-communicatiedienst aangeboden door de operator aan de abonnee die geen elektronische-communicatiebetaaldienst is;

3° "directe identificatiemethode": de methode waarbij de operator voor de behoeften van de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid:

— 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 een rechtspersoon die abonnee is van de operator om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval;

— een kopie van het identificatiedocument van deze natuurlijke persoon verzamelt en bewaart;

4° "indirecte identificatiemethode": de 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;

5° "verkooppunt": het fysiek verkooppunt van voorafbetaalde kaarten of abonnementen van een operator.

§ 3. De operator die een elektronische-communicatiebetaaldienst verstrekt, identificeert zijn abonnees door middel van een directe of indirecte identificatiemethode, met uitzondering van de indirecte identificatiemethodes bedoeld in paragraaf 10, eerste lid, 1° en 2°.

In afwijking van het tweede lid mag de in dat lid bedoelde operator de abonnee ook identificeren aan de hand van de indirecte identificatiemethode bedoeld in paragraaf 10, eerste lid, 2°, wanneer hij elektronische-communicatiediensten aanbiedt waarvoor de directe en indirecte identificatiemethodes bedoeld in het tweede lid belangrijke lasten met zich meebrengen voor de abonnees en de operator, namelijk:

— de vaste internettoegangsdiensten die worden gebruikt door natuurlijke personen buiten hun verblijfplaats en de plaats waar ze een beroepsactiviteit uitoefenen, zoals de elektronische-communicatiediensten die worden verstrekt door middel van WiFi hotspots van de operatoren;

— de andere diensten bepaald door de Koning.

Een operator die een gratis elektronische-communicatiedienst verstrekt, identificeert zijn abonnees aan de hand van een indirecte identificatiemethode zoals bedoeld in paragraaf 10.

§ 4. Het is verboden voor de verkooppunten om identificatiegegevens of kopieën van identiteitsdocumenten te bewaren, of deze voor enig ander doeleinde te gebruiken dan de identificatie van de abonnee.

De operatoren nemen de gepaste en evenredige technische en organisatorische maatregelen voor de tenuitvoerlegging van het in het eerste lid bedoelde verbod, door onder andere de verkooppunten toe te staan om de identificatiegegevens en de kopieën van identificatiedocumenten rechtstreeks in te voeren in hun computersystemen.

Indien een rechtstreekse invoer in de computersystemen van de operator tijdelijk niet mogelijk is door een storing in deze systemen, worden de identificatiegegevens en de kopieën van identificatiedocumenten die het verkooppunt op het moment van de storing heeft bewaard, vernietigd, uiterlijk na de activering van de elektronische-communicatiedienst.

Behoudens andersluidende wettelijke bepaling, worden de identificatiegegevens en de kopieën van identificatiedocumenten vergaard krachtens dit artikel bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de stopzetting van de elektronische-communicatiedienst.

La personne qui distribue en Belgique ces cartes prépayées, ces abonnements ou ces objets connectés fournit aux officiers de police judiciaire de l'Institut, à leur demande, la preuve de cet accord.

En cas d'accord de l'entreprise, cette dernière est opérateur et se conforme à l'article 9, § 1er.

§ 2. Pour l'application du présent article, il faut entendre par:

1° "service de communications électroniques payant": le service de communications électroniques pour lequel un paiement de l'abonné à l'opérateur est nécessaire pour utiliser le service ou continuer à l'utiliser, ainsi que tout service de communications électroniques offert sans surcoût par l'opérateur à l'abonné conjointement à ce service;

2° "service de communications électroniques gratuit": le service de communications électroniques offert par l'opérateur à l'abonné autre que le service de communications électroniques payant;

3° "méthode d'identification directe": la méthode par laquelle l'opérateur collecte et conserve pour les besoins des autorités visées à l'article 127/1, § 3, alinéa 1er:

— des données fiables relatives à l'identité civile d'une personne physique, qui est son abonné ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir l'obligation d'identification de la personne morale et, le cas échéant;

— une copie du document d'identification de cette personne physique;

4° "méthode d'identification indirecte": la méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés;

5° "point de vente": le point de vente physique de cartes prépayées ou d'abonnements d'un opérateur.

§ 3. L'opérateur qui fournit un service de communications électroniques payant identifie ses abonnés au moyen d'une méthode d'identification directe ou indirecte, à l'exception des méthodes d'identification indirecte visées au paragraphe 10, alinéa 1er, 1° et 2°.

Par dérogation à l'alinéa 2, l'opérateur visé à cet alinéa peut également identifier l'abonné au moyen de la méthode d'identification indirecte visée au paragraphe 10, alinéa 1er, 2°, lorsqu'il offre un service de communications électroniques pour lequel les méthodes d'identification directe et indirecte autorisées par l'alinéa 2 impliquent des contraintes importantes pour les abonnés et l'opérateur, à savoir:

— les services fixes d'accès à internet utilisés par des personnes physiques en dehors de leur lieu de résidence et du lieu où elles exercent une activité professionnelle, tels que les services de communications électroniques offerts à l'aide de bornes WiFi des opérateurs;

— les autres services déterminés par le Roi.

L'opérateur qui fournit un service de communications électroniques gratuit identifie ses abonnés au moyen d'une méthode d'identification indirecte visée au paragraphe 10.

§ 4. Il est interdit aux points de vente de conserver des données d'identification ou des copies de documents d'identification ou d'en faire un usage quelconque autre que l'identification de l'abonné.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour la mise en œuvre de l'interdiction visée à l'alinéa 1er, en ce compris en permettant aux points de vente d'introduire directement les données d'identification et les copies de documents d'identification dans leurs systèmes informatiques.

Si une introduction directe dans les systèmes informatiques de l'opérateur n'est temporairement pas possible en raison d'une défaillance de ces systèmes, les données d'identification et les copies de documents d'identification gardées par le point de vente lors de cette défaillance sont détruites au plus tard après l'activation du service de communications électroniques.

Sauf disposition légale contraire, les données d'identification et les copies de document d'identification collectées en vertu du présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la fin du service de communications électroniques.

§ 5. De operator stelt alles in het werk om de betrouwbaarheid van de identificatie van de abonnee die een natuurlijke persoon is te garanderen.

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, vergewist hij zich ervan:

— dat de vergaarde identificatiegegevens overeenstemmen met de gegevens op het document;

— dat de geldigheidsdatum van dat document niet overschreden is op het ogenblik van de identificatie van de abonnee.

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, stelt hij alles in het werk om te controleren:

— of het document het origineel is, leesbaar is en de indruk geeft van authenticiteit;

— dat dit document betrekking heeft op de geïdentificeerde persoon.

Teneinde de betrouwbaarheid bedoeld in het eerste lid te garanderen en identiteitsfraudes te vermijden, kan de operator of het verkooppunt automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identificatiedocument van de abonnee en deze van zijn gezicht, volgens deze voorwaarden:

1° de vergelijkingstool werd toegestaan door de minister en de minister van Justitie, na verificatie dat deze tool de betrouwbaarheid van de identificatie van de abonnee voor de behoeften van de autoriteiten garandeert, in het bijzonder rekening houdende met het risico van identiteitsfraude vanwege de persoon die zich identificeert;

2° de operator biedt de abonnee minstens een alternatieve manier aan om zich te identificeren;

3° de abonnee heeft zijn uitdrukkelijke instemming gegeven in de zin van artikel 4,11), van de AVG, wat met name inhoudt dat de abonnee op de hoogte is van de doeleinden waarvoor deze gegevens zullen worden verzameld, te weten de tenuitvoerbrenging van de wettelijke verplichting tot identificatie van de abonnee op betrouwbare wijze en de strijd tegen identiteitsfraude;

4° de operator en het verkooppunt mogen deze biometrische gegevens niet meedelen aan een derde als bedoeld in artikel 4, 10), van de AVG en zij mogen deze maar verwerken binnen de grenzen van wat nodig is om de in dit lid beoogde doeleinden van gezichtsvergelijking te verwezenlijken;

5° het is verboden om deze biometrische gegevens te bewaren na die vergelijking.

Wanneer de abonnee zich aan de hand van een Belgische elektronische identiteitskaart identificeert en de operator de in het vierde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast, kan de operator aan de abonnee vragen om de pincode in te tikken.

§ 6. De toegestane identificatiedocumenten ter identificatie van de abonnee die een natuurlijke persoon is, zijn de volgende:

1° de Belgische elektronische identiteitskaart;

2° het Belgisch paspoort;

3° het bewijs van inschrijving in het vreemdelingenregister – tijdelijk verblijf, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (A-kaart);

4° de beperkte verblijfstitel (A-kaart);

5° het bewijs van inschrijving in het vreemdelingenregister, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (B-kaart);

6° de onbeperkte verblijfstitel (B-kaart);

7° de identiteitskaart voor vreemdelingen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (C-kaart);

8° de vestigingsvergunning (K-kaart);

9° de EU-verblijfstitel voor langdurig ingezetenen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (D-kaart);

10° de EU-verblijfstitel voor langdurig ingezetenen (L-kaart);

11° de verklaring van inschrijving, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E-kaart);

12° het document van inschrijving "Art 8 RL 2004/38/EG" E (EU-kaart);

13° het document ter staving van duurzaam verblijf, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E+-kaart);

14° het document van duurzaam verblijf "Art 19 RL 2004/38/EG" (EU+-kaart);

§ 5. L'opérateur met tout en œuvre pour assurer la fiabilité de l'identification de l'abonné qui est une personne physique.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il s'assure:

— que les données d'identification collectées correspondent aux données sur ce document;

— que la date de validité de ce document n'est pas dépassée au moment de l'identification de l'abonné.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il met tout en œuvre pour vérifier:

— que ce document est l'original, lisible et présente l'apparence d'authenticité;

— que ce document est relatif à la personne identifiée.

Afin d'assurer la fiabilité visée à l'alinéa 1er et d'éviter les fraudes à l'identité, l'opérateur ou le point de vente peut réaliser de manière automatique une comparaison entre les paramètres biométriques sur la photo du document d'identification de l'abonné et ceux de son visage, aux conditions suivantes:

1° l'outil de comparaison a été autorisé par le ministre et le ministre de la Justice, après vérification que cet outil assure la fiabilité de l'identification de l'abonné pour les besoins des autorités, en tenant compte en particulier du risque de fraude à l'identité de la part de la personne qui s'identifie;

2° l'opérateur offre à l'abonné au moins une manière alternative de s'identifier;

3° l'abonné a donné son consentement explicite au sens de l'article 4, 11), du RGPD, ce qui implique notamment que l'abonné soit informé des finalités pour lesquelles ces données seront récoltées, à savoir la mise en œuvre de l'obligation légale d'identification de l'abonné de manière fiable et la lutte contre la fraude à l'identité;

4° l'opérateur et le point de vente ne peuvent communiquer ces données biométriques à un tiers au sens de l'article 4, 10), du RGPD et ne peuvent les traiter que dans les limites nécessaires en vue d'accomplir les finalités de comparaison faciale visées au présent alinéa;

5° il est interdit de conserver ces données biométriques au-delà de cette comparaison.

Lorsque l'abonné s'identifie à l'aide d'une carte d'identité électronique belge et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 4, l'opérateur peut demander à l'abonné l'introduction du code PIN.

§ 6. Les documents d'identification qui sont admis pour identifier l'abonné qui est une personne physique sont les suivants:

1° la carte d'identité électronique belge;

2° le passeport belge;

3° le certificat d'inscription au registre des étrangers – séjour temporaire, délivré avant le 11 octobre 2021, en cours de validité (carte A);

4° le titre de séjour limité (carte A);

5° le certificat d'inscription au registre des étrangers, délivré avant le 11 octobre 2021, en cours de validité (carte B);

6° le titre de séjour illimité (carte B);

7° la carte d'identité d'étranger, délivrée avant le 11 octobre 2021, en cours de validité (carte C);

8° le titre d'établissement (carte K);

9° le titre de séjour de résident de longue durée – UE, délivré avant le 11 octobre 2021, en cours de validité (carte D);

10° le titre de séjour de résident de longue durée – UE (carte L);

11° l'attestation d'enregistrement, délivrée avant le 10 mai 2021, en cours de validité (carte E);

12° le document d'enregistrement "Art 8 DIR 2004/38/CE" E (carte EU);

13° le document attestant de la permanence de séjour, délivré avant le 10 mai 2021, en cours de validité (carte E+);

14° le document de séjour permanent "Art 19 DIR 2004/38/CE" (carte EU+);

15° de verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F-kaart);

16° de verblijfskaart van een familielid van een burger van de Unie "familielid EU - Art 10 RL 2004/38/EG" (F-kaart);

17° de duurzame verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F+-kaart);

18° de duurzame verblijfskaart van een familielid van een burger van de Unie "Familielid EU – Art 20 RL 2004/38/EG" (F+-kaart);

19° de Europese blauwe kaart (H-kaart);

20° de vergunning voor een binnen een onderneming overgeplaatste persoon "ICT" (I-kaart);

21° de vergunning voor lange-termijnmobiliteit "mobiele ICT" (J-kaart);

22° de verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

23° de duurzame verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

24° de kaart voor klein grensverkeer voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU – grensarbeider" (N-kaart);

25° de akte van bekendheid;

26° de bijlage 12 verstrekt krachtens artikel 6 van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten of krachtens artikel 36*bis* van het koninklijk besluit van 8 oktober 1981 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

27° het attest van immatriculatie (oranje kaart);

28° de buitenlandse identiteitskaart, wanneer een internationaal paspoort niet nodig is om in België te verblijven;

29° de bijzondere identiteitskaarten verstrekt aan de categorieën van personeel dat actief is in diplomatieke en consulaire zendingen en aan hun familieleden, krachtens de Verdragen van Wenen van 1961 en 1963 en het koninklijk besluit van 30 oktober 1991 betreffende de documenten voor het verblijf in België van bepaalde vreemdelingen;

30° de identiteitskaart verstrekt conform de Conventies van Genève van 12 augustus 1949 inzake de bescherming van de slachtoffers van internationale gewapende conflicten;

31° het buitenlands paspoort;

32° elk ander document bepaald door de Koning, op voorwaarde dat het koninklijk besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren die over verkooppunten beschikken, maken het voor hun abonnees mogelijk om zich te identificeren aan de hand van om het even welke van de in het eerste lid bedoelde identificatiedocumenten, in het kader van minstens één identificatiemethode van hun keuze.

In afwijking van het tweede lid kan een operator weigeren om een abonnee te identificeren op basis van een ander identificatiedocument dat is vermeld in het eerste lid dan de Belgische elektronische identiteitskaart indien hij hem de mogelijkheid biedt zich te identificeren op een van de alternatieve wijzen vermeld in 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 en voor zover de abonnee in staat is die alternatieve wijze te gebruiken.

Wanneer de operator een abonnee identificeert uitgaande van een identificatiedocument, bewaart hij een kopie van dat document, behalve als het gaat om de Belgische elektronische identiteitskaart.

De operatoren nemen de passende en evenredige maatregelen van technische en organisatorische aard teneinde te verhinderen dat de verkooppunten of derden een kopie nemen van de Belgische elektronische identiteitskaart, zulks onverminderd paragraaf 4, derde lid.

§ 7. Onverminderd artikel 126 bewaart de operator het rijksregisternummer, de naam en voornaam van zijn abonnee die een natuurlijke persoon is, wanneer hij die abonnee identificeert aan de hand van zijn Belgische elektronische identiteitskaart.

15° la carte de séjour de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F);

16° la carte de séjour de membre de la famille d'un citoyen de l'Union "membre famille UE - Art 10 DIR 2004/38/CE" (carte F);

17° la carte de séjour permanent de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F+);

18° la carte de séjour permanent de membre de la famille d'un citoyen de l'Union "membre famille UE – Art 20 DIR 2004/38/CE" (carte F+);

19° la carte bleue européenne (carte H);

20° le permis pour personne faisant l'objet d'un transfert temporaire intragroupe "ICT" (carte I);

21° le permis pour mobilité de longue durée "mobile ICT" (carte J);

22° la carte de séjour pour bénéficiaires de l'accord de retrait "Art. 50 TUE" (carte M);

23° la carte de séjour permanent pour bénéficiaires de l'accord de retrait "Art. 50 TUE" (carte M);

24° la carte pour petit trafic frontalier pour bénéficiaires de l'accord de retrait "Art. 50 TUE – Travailleur frontalier" (carte N);

25° l'acte de notoriété;

26° l'annexe 12 délivrée en application de l'article 6 de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité ou en application de l'article 36*bis* de l'arrêté royal du 8 octobre 1981 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;

27° l'attestation d'immatriculation (carte orange);

28° la carte d'identité étrangère, lorsqu'un passeport international n'est pas nécessaire pour séjourner en Belgique;

29° les cartes d'identité spéciales délivrées aux catégories de personnel actives dans les missions diplomatiques et consulaires et aux membres de leur famille, en vertu des Conventions de Vienne de 1961 et 1963 et de l'arrêté royal du 30 octobre 1991 relatif aux documents de séjour en Belgique de certains étrangers;

30° la carte d'identité délivrée conformément aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux;

31° le passeport étranger;

32° tout autre document déterminé par le Roi, pour autant que l'arrêté royal soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs qui disposent de points de vente permettent à leurs abonnés de s'identifier à l'aide de n'importe lequel des documents d'identification visés à l'alinéa 1er, dans le cadre d'au moins une méthode d'identification de leur choix.

Par dérogation à l'alinéa 2, un opérateur peut refuser d'identifier un abonné sur base d'un document d'identification visé à l'alinéa 1er autre que la carte d'identité électronique belge s'il lui offre la possibilité de s'identifier selon une des manières alternatives visées à l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée et pour autant que l'abonné soit en mesure de mettre en œuvre cette alternative.

Lorsqu'un opérateur identifie l'abonné à partir d'un document d'identification, il conserve une copie de ce document, sauf lorsqu'il s'agit de la carte d'identité électronique belge.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour empêcher que les points de vente ou des tiers ne prennent une copie de la carte d'identité électronique belge, sans préjudice du paragraphe 4, alinéa 3.

§ 7. Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné qui est une personne physique à partir de sa carte d'identité électronique belge, il conserve son numéro de registre national, son nom et son prénom.

Onverminderd artikel 126 bewaart de operator, bij het identificeren van de abonnee via een ander document dan de Belgische elektronische identiteitskaart of aan de hand van een andere directe identificatiemethode dan de overlegging van een identificatiedocument, tussen de volgende gegevens diegene die op het voorgelegde identificatiedocument staan of diegene die worden verwerkt tijdens de toepassing van de directe identificatiemethode:

1° de naam en voornaam;

2° de nationaliteit;

3° de geboortedatum;

4° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

5° het nummer van het identificatiedocument en het land van uitgifte van het document wanneer het een buitenlands document betreft;

6° het verband tussen de nieuwe elektronische-communicatiedienst waarop de abonnee intekent en de dienst waarvoor hij reeds werd geïdentificeerd.

§ 8. Wanneer een operator op basis van een voorafbetaalde kaart een mobiele elektronische-communicatiedienst aanbiedt aan een abonnee die een rechtspersoon is en die hij identificeert aan de hand van een directe identificatiemethode, vergaart en bewaart hij de burgerlijke identiteit van een natuurlijke persoon die handelt voor rekening van de rechtspersoon, conform de vereisten bedoeld in de paragrafen 4 tot 7.

§ 9. Wat de directe identificatiemethodes betreft, kan de Koning:

1° de enige methodes vastleggen die de operatoren mogen gebruiken;

2° per methode bepalen aan welke voorwaarden moet worden voldaan, onder meer door een door een onderneming voorgestelde identificatiemethode te onderwerpen aan een voorafgaande machtiging van de minister en van de minister van Justitie;

3° verplichtingen opleggen aan de operatoren, aan de verkooppunten, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 10. De operator maakt het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk om zijn abonnees te identificeren via een indirecte identificatiemethode:

1° door de bewaring, overeenkomstig artikel 126 en gedurende de in dat artikel bepaalde termijnen, van het IP-adres dat werd gebruikt om zich op de elektronische-communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden, of;

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 dit artikel, of;

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, en;

— de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die de abonnee van de operator is of die handelt voor rekening van een rechtspersoon die de abonnee van de operator is, teneinde zijn verplichtingen inzake identificatie te vervullen, of;

4° in geval van een simkaart ("subscriber identity/identification module") of andere gelijkwaardige kaart die in een voertuig wordt ingebouwd, door de vergaring en bewaring van het chassisnummer van het voertuig en van de link tussen het chassisnummer en het nummer van de kaart;

5° in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, 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, zijnde het door de Dienst Vreemdelingenzaken toegekende dossiernummer, en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden, of:

Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné à partir d'un autre document que la carte d'identité électronique belge ou au moyen d'une autre méthode d'identification directe que la présentation d'un document d'identification, il conserve parmi les données suivantes celles qui se trouvent sur le document d'identification présenté ou qui sont traitées lors de la mise en œuvre de la méthode d'identification directe:

1° le nom et le prénom;

2° la nationalité;

3° la date de naissance;

4° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone;

5° le numéro du document d'identification et le pays d'émission du document lorsqu'il s'agit d'un document étranger;

6° le lien entre le nouveau service de communications électroniques auquel l'abonné souscrit et le service pour lequel il a déjà été identifié.

§ 8. Lorsqu'un opérateur fournit à un abonné qui est une personne morale un service de communications électroniques mobile sur la base d'une carte prépayée et qu'il l'identifie par le biais d'une méthode d'identification directe, il collecte et conserve, en respectant les exigences visées aux paragraphes 4 à 7, l'identité civile d'une personne physique qui agit pour le compte de la personne morale.

§ 9. Pour ce qui concerne les méthodes d'identification directe, le Roi peut:

1° déterminer les seules méthodes que les opérateurs peuvent utiliser;

2° prévoir, par méthode, les conditions à respecter, en ce compris soumettre une méthode d'identification proposée par une entreprise à une autorisation préalable du ministre et du ministre de la Justice;

3° imposer des obligations aux opérateurs, aux points de vente, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 10. L'opérateur permet aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'identifier ses abonnés par le biais d'une méthode d'identification indirecte:

1° en conservant, en exécution de l'article 126 et pendant les délais prévus par cet article, l'adresse IP ayant servi à la souscription au service de communications électroniques ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées avec ces adresses, ou;

2° en collectant et conservant le numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément au présent article, ou;

3° en cas de paiement en ligne spécifique à la souscription d'un service de communications électroniques, en collectant et conservant:

— la référence de l'opération de paiement, et;

— le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir son obligation en matière d'identification, ou;

4° en cas de carte SIM ("subscriber identity/identification module") ou toute autre carte équivalente intégrée dans un véhicule, en collectant et conservant le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte;

5° en cas de souscription d'un abonné qui réside dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, en collectant et conservant le nom et le prénom de l'abonné, son numéro de sécurité publique, à savoir le numéro de dossier attribué par l'Office des Etrangers et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu, ou;

6° in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, door de vergaring en bewaring van de precieze benaming van de rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals een rijksregisternummer, welke hem wordt meegedeeld door de rechtspersoon.

Voor de toepassing van het eerste lid, 6°:

1° moet de rechtspersoon, alvorens te kunnen intekenen op een elektronische-communicatiedienst voor de natuurlijke persoon, een erkenning verkrijgen, verstrekt door de minister en de minister van Justitie, en met als voorwerp om na te gaan dat de persoon de democratische waarden vastgelegd in de Grondwet alsook dit artikel nakomt;

2° identificeert de rechtspersoon zich bij de operator overeenkomstig dit artikel;

3° identificeert de rechtspersoon de abonnees aan de hand van een van de identificatiedocumenten bedoeld in paragraaf 6, conform de vereisten inzake betrouwbaarheid bedoeld in paragraaf 5, of aan de hand van een andere methode die toegestaan is in de in de bepaling onder 1° bedoelde erkenning;

4° bewaart de rechtspersoon een kopie van het andere identificatiedocument van de abonnees dan de Belgische elektronische identiteitskaart, behoudens afwijking toegestaan in de in de bepaling onder 1° bedoelde erkenning;

5° bewaart de rechtspersoon een geactualiseerde lijst aan de hand waarvan het verband kan worden vastgesteld tussen de elektronische-communicatiedienst en de abonnees, met daarin ten minste de naam, de voornaam, het verblijfadres als de persoon dat heeft, de geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals het rijksregisternummer.

De Koning kan:

1° per in het eerste lid vermelde methode de voorwaarden vastleggen die moeten worden nageleefd, waarbij een voorwaarde het verkrijgen van een voorafgaande machtiging van de minister en van de minister van Justitie kan zijn;

2° verplichtingen opleggen aan de operatoren, aan de in het eerste lid bedoelde rechtspersonen, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 11. Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

De Koning, voor de mobiele elektronische-communicatiediensten verstrekt op basis van een voorafbetaalde kaart:

1° beperkt de mogelijkheid voor de abonnee om derden gebruik te laten maken van de dienst;

2° legt verplichtingen op aan de abonnees die rechtspersonen zijn om de gewoonlijke gebruikers van de dienst te identificeren.

De operator die een simkaart of een gelijkwaardige kaart aanbiedt die bestemd is om in een voertuig te worden ingebouwd, bewaart het chassisnummer van dat voertuig, evenals de link tussen het chassisnummer en het nummer van deze kaart. Op verzoek van een autoriteit deelt de operator haar enkel dat chassisnummer of het nummer van deze kaart mee.

De Koning kan de nadere regels van de verplichting bedoeld in het derde lid vastleggen en kan de ondernemingen die over het chassisnummer beschikken, verplichten om dat door te geven aan de operatoren.

§ 12. Indien een operator niet voldoet aan de hem door dit artikel of door de Koning opgelegde maatregelen, is het hem verboden de dienst waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.

De operatoren sluiten de abonnees die niet voldoen aan de hen door dit artikel of door de Koning opgelegde maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die abonnees worden op geen enkele wijze vergoed voor de afsluiting.

Het koninklijk besluit bedoeld in dit artikel wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en wordt vastgesteld na overleg in de Ministerraad.".

6° en cas de souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à effectuer cette souscription, en collectant et conservant la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée, tel un numéro de registre national, ces informations lui étant transmises par cette personne morale.

Pour l'application de l'alinéa 1er, 6°, la personne morale:

1° doit, avant de pouvoir souscrire à un service de communications électroniques pour la personne physique, obtenir un agrément, délivré par le ministre et le ministre de la Justice, et ayant pour objet de vérifier qu'elle respecte les valeurs démocratiques inscrites dans la Constitution ainsi que le présent article;

2° s'identifie auprès de l'opérateur conformément au présent article;

3° identifie les abonnés à l'aide d'un des documents d'identification visés au paragraphe 6, conformément aux exigences de fiabilité visées au paragraphe 5, ou à l'aide d'une autre méthode autorisée dans l'agrément visé au 1°;

4° conserve une copie du document d'identification des abonnés autre que la carte d'identité électronique belge, sauf dérogation accordée dans l'agrément visé au 1°;

5° conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le prénom, l'adresse de la résidence, lorsque la personne en dispose, la date de naissance et le numéro par lequel elle est identifiée, tel le numéro de registre national.

Le Roi peut:

1° prévoir par méthode visée à l'alinéa 1er les conditions à respecter, une condition pouvant être l'obtention d'une autorisation préalable du ministre et du ministre de la Justice;

2° imposer des obligations aux opérateurs, aux personnes morales visées à l'alinéa 1er, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 11. Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Pour les services de communications électroniques mobiles fournis au moyen d'une carte prépayée, le Roi:

1° restreint la possibilité pour l'abonné de permettre à des tiers de bénéficier du service;

2° impose des obligations aux abonnés qui sont des personnes morales afin de déterminer les utilisateurs habituels du service.

L'opérateur qui offre une carte SIM ou toute carte équivalente, destinée à être intégrée dans un véhicule, conserve le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte. À la demande d'une autorité, l'opérateur ne lui communique que ce numéro de châssis ou le numéro de cette carte.

Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent du numéro de châssis de le transmettre aux opérateurs.

§ 12. Si un opérateur ne respecte pas les mesures qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les abonnés qui ne respectent pas les mesures qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces abonnés ne sont en aucune manière indemnisés pour la déconnexion.

L'arrêté royal visé dans le présent article est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres.".

Art. 13. In dezelfde wet wordt een artikel 127/1 ingevoegd, luidende:

"Art. 127/1. § 1. Voor de toepassing van dit artikel omvat zware criminaliteit met name de feiten waarvoor er ernstige aanwijzingen bestaan:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.

Enkel de autoriteiten bedoeld in paragraaf 2 mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127, voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.

In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.

Art. 13. Dans la même loi, il est inséré un article 127/1, rédigé comme suit:

"Art 127/1. § 1er. Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 4. De gegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1° tot 3° en 6°.

Enkel de in paragraaf 2, 1° tot 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens de artikelen 126/1 en 126/3 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

§ 5. De formele wettelijke norm van Belgisch recht bedoeld in de paragrafen 2 tot 4 preciseert:

— de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;

— de categorieën van gegevens die mogen gevraagd worden;

— de beoogde doeleinden;

— de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.

De minister laat in het *Belgisch Staatsblad* een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127.

Op het verzoek van de minister of van het Instituut verstrekken de Belgische autoriteiten bedoeld in de paragrafen 2 tot 4 de informatie die nodig is om deze omzendbrief op te stellen.

§ 6. De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127, omvatten de volgende minimale vermeldingen:

1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;

2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;

3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;

4° de gewenste antwoordtermijn.

§ 7. Het Instituut stuurt jaarlijks aan de minister en de minister van Justitie statistieken over de verstrekking aan de autoriteiten van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127. Deze ministers sturen die jaarlijks door naar de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name:

1° de gevallen waarin bewaarde gegevens zijn verstrekt aan de bevoegde autoriteiten overeenkomstig de toepasselijke wettelijke bepalingen;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om bewaarde gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens noch vertrouwelijke informatie omvatten.

De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90decies van het Wetboek van strafvordering uitbrengt aan het Parlement.

Het Instituut vraagt aan de operatoren en aan de door de Koning aangewezen dienst de informatie aan de hand waarvan het de in het eerste lid bedoelde verplichting kan vervullen.”.

Art. 14. In dezelfde wet wordt een artikel 127/2 ingevoegd, luidende:

“Art. 127/2. § 1. De operatoren garanderen de kwaliteit van de bewaarde metagegevens van elektronische communicatie en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ze ervoor dat ze dezelfde kwaliteit hebben als de gegevens die worden verwerkt in het kader van de verstrekking van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst.

De operatoren stellen alles in het werk om de technische verbanden te leggen tussen de gegevens bewaard voor de autoriteiten die nodig zijn om op hun vragen te antwoorden.

§ 4. Les données conservées en vertu des articles 126/1 et 126/3 le sont pour les autorités et finalités visées au paragraphe 2, 1° à 3° et 6°.

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

§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise:

— la ou les catégories d’entreprises auxquelles l’autorité peut demander des données;

— les catégories de données qui peuvent être demandées;

— les finalités poursuivies;

— les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.

Le ministre fait publier au *Moniteur belge* une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d’un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127.

À la demande du ministre ou de l’Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.

§ 6. Les demandes que les autorités adressent aux opérateurs afin d’obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes:

1° l’identité de l’autorité demanderesse, ou, lorsque la demande est envoyée à l’opérateur par un service central pour le compte de cette autorité, l’identité de ce service;

2° la fonction de la personne de contact auprès de l’autorité demanderesse, ou, lorsque la demande est envoyée à l’opérateur par un service central pour le compte de l’autorité, la fonction de la personne de contact auprès de ce service central;

3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l’opérateur par le biais d’un service central pour le compte d’une autre autorité;

4° le délai de réponse souhaité.

§ 7. L’Institut transmet annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment:

1° les cas dans lesquels des données conservées ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données conservées n’ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l’information confidentielle.

Les données qui concernent l’application de l’alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice fait au Parlement conformément à l’article 90decies du Code d’instruction criminelle.

L’Institut demande aux opérateurs et au service désigné par le Roi les informations qui lui permettent de remplir l’obligation visée à l’alinéa 1er.”.

Art. 14. Dans la même loi, il est inséré un article 127/2, rédigé comme suit:

“Art. 127/2. § 1er. Les opérateurs veillent à garantir la qualité des métadonnées de communications électroniques conservées et, pour ce qui concerne les données conservées pour les autorités, à ce qu’elles soient de la même qualité que les données traitées dans le cadre de la fourniture du réseau ou du service de communications électroniques.

Les opérateurs mettent tout en œuvre pour établir les liens techniques entre les données conservées pour les autorités qui sont nécessaires pour répondre à leurs demandes.

§ 2. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie, bewaard voor de autoriteiten:

1° garanderen de operatoren dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk of verwerkt door de dienst;

2° nemen de operatoren maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

3° mogen de operatoren de bewaarde gegevens niet gebruiken voor andere doeleinden dan de verstrekking van deze gegevens aan de autoriteiten, tenzij wanneer ze de toestemming krijgen van de betrokken abonnees, conform artikel 4, 11), van de AVG en onverminderd andere wettelijke bepalingen.

§ 3. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie dienen de operatoren:

1° de gegevens op het grondgebied van de Europese Unie te bewaren en in België de door een Belgische autoriteit gevraagde gegevens te verstrekken;

2° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager worden verwijderd of dat deze gegevens worden geanonimiseerd;

3° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij onbedoeld hetzij onrechtmatig, tegen een onbedoeld verlies of onbedoelde wijziging of tegen niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 107/2;

4° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 127/3, § 1, op manuele of op geautomatiseerde wijze;

5° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord.

§ 4. De in de paragraaf 3, 5°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.

De operator neemt de nodige maatregelen opdat elke raadpleging van de gegevens die hij bewaart voor de autoriteiten, automatisch in het logboek een registratie van de volgende gegevens genereert: de identiteit van de persoon die de gegevens heeft geraadpleegd, het moment van de raadpleging en de geraadpleegde gegevens.

Dit logboek bevat eveneens de volgende informatie en documenten, die eventueel manueel daarin worden ingevoerd:

1° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek, een kopie van het verzoek of een link naar dit laatste;

2° wat betreft het antwoord van de operator op het verzoek van de autoriteit: de identiteit van zijn geadresseerde, de datum en het tijdstip van de verzending ervan alsook het communicatiemiddel dat werd gebruikt voor de verzending.

Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.

De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.

De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen. Elke wijziging van de in het logboek opgenomen gegevens is verboden. Elke raadpleging van het logboek wordt geregistreerd.

De Koning kan, na advies van de Gegevens-beschermingsautoriteit en van het Instituut, de eisen bepalen die de operatoren in acht moeten nemen wat betreft het logboek.

In het kader van de controle van de operator mogen het Instituut alsook de inspecteur-generaal en de door de inspecteur-generaal aangewezen inspecteurs binnen de Gegevensbeschermingsautoriteit, bedoeld in artikel 66, § 1, van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.

§ 2. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, conservées pour les autorités, les opérateurs:

1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ou traitées par le service;

2° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

3° ne peuvent utiliser les données conservées pour d'autres finalités que la fourniture de ces données aux autorités, sauf lorsqu'ils obtiennent le consentement des abonnés concernés conformément à l'article 4, 11), du RGDP et sans préjudice d'autres dispositions légales.

§ 3. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, les opérateurs:

1° conservent les données sur le territoire de l'Union européenne et fournissent en Belgique les données demandées par une autorité belge;

2° veillent à ce que les données conservées soient détruites de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou que ces données soient rendues anonymes;

3° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, conformément à l'article 107/2;

4° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 127/3, § 1er, de manière manuelle ou automatisée;

5° assurent une traçabilité de l'exploitation des données conservées.

§ 4. La traçabilité visée au paragraphe 3, 5°, s'effectue à l'aide d'un journal.

L'opérateur prend les mesures nécessaires pour que chaque consultation des données qu'il conserve pour les autorités génère de manière automatisée un enregistrement dans le journal des données suivantes: l'identité de la personne ayant consulté les données, le moment de la consultation et les données consultées.

Ce journal comprend également les informations et documents suivants, qui, le cas échéant, y sont introduits de manière manuelle:

1° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande, une copie de la demande ou un lien vers cette dernière;

2° pour ce qui concerne la réponse de l'opérateur à la demande de l'autorité: l'identité de son destinataire, la date et l'heure de son envoi ainsi que le moyen de communication utilisé pour l'envoyer.

Le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte.

Les données de ce journal sont conservées pendant une période de dix ans. À l'échéance de la période de conservation, les données du journal sont détruites.

L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal. Toute modification des données reprises dans le journal est interdite. Toute consultation du journal est journalisée.

Le Roi peut préciser, après avis de l'Autorité de protection des données et de l'Institut, les exigences à respecter par les opérateurs concernant le journal.

Dans le cadre du contrôle de l'opérateur, l'Institut ainsi que l'inspecteur général et les inspecteurs désignés par l'inspecteur général, au sein de l'Autorité de protection des données, visés à l'article 66, § 1er, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.

§ 5. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2, 3 of 4, dan kan het de operator verplichten om zich te onderwerpen aan een veiligheidscontrole door een gekwalificeerde onafhankelijke instantie die de operator ter goedkeuring voorlegt aan het Instituut.

Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 4.

Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.".

Art. 15. In dezelfde wet wordt een artikel 127/3 ingevoegd, luidende:

"Art. 127/3. § 1. Bij elke operator wordt een Coördinatie-cel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.

Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.

Deze autoriteiten richten hun verzoeken tot deze cel.

In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval neemt elke operator de nodige maatregelen opdat deze gemeenschappelijke Coördinatiecel in staat is om te antwoorden op de verzoeken die eraan worden gericht.

De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten waaraan de Coördinatiecel moet beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid.

§ 2. De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim. Deze leden delen aan de aangestelden enkel de gegevens mee die strikt noodzakelijk zijn om die bijstand te krijgen.

Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.

De leden van de Coördinatiecel beschikken over een positief en niet-achterhaald veiligheidsadvies bedoeld in artikel 22*quinquies*/1 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

De administratieve instantie die bevoegd is voor de behandeling van de adviezen is de minister van Justitie.

De Koning bepaalt alternatieve veiligheidsmaatregelen die passend zijn voor de personen voor wie een veiligheidsadvies niet kan worden verstrekt wegens gebrek aan voldoende informatie.

In afwijking van het derde lid kan een in het vijfde lid bedoelde persoon deel uitmaken van de Coördinatiecel, wanneer deze alternatieve veiligheidsmaatregelen in acht worden genomen en zonder over een veiligheidsadvies te beschikken.

De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende:

1° voor de andere operatoren dan diegene die reeds over een veiligheidsofficier beschikken wegens andere activiteiten dan de Coördinatiecel, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een dergelijke officier aan te stellen in functie van het aantal verzoeken ontvangen vanwege de gerechtelijke autoriteiten, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inzonderheid wat het gebruik van de talen betreft;

3° de regels voor de toegang van de gemachtigde Belgische autoriteiten tot de contactgegevens van de Coördinatiecel en zijn leden.

§ 5. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2, 3 ou 4, il peut l'obliger à se soumettre à un contrôle de sécurité effectué par un organisme qualifié indépendant, proposé par l'opérateur à l'Institut pour accord.

Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en ce compris le journal visé au paragraphe 4.

Le rapport et les résultats de ce contrôle de sécurité sont communiqués à l'Institut. Le coût du contrôle est à la charge de l'opérateur.".

Art. 15. Dans la même loi, il est inséré un article 127/3, rédigé comme suit:

"Art. 127/3. § 1er. Auprès de chaque opérateur est constituée une Cellule de coordination, chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques.

Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur.

Ces autorités adressent leurs demandes à cette cellule.

Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, chaque opérateur prend les mesures nécessaires pour que cette Cellule de coordination commune soit en mesure de répondre aux demandes qui lui sont adressées.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité.

§ 2. Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel. Ces membres ne communiquent aux préposés que les données strictement nécessaires pour obtenir cette aide.

Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.

Les membres de la Cellule de coordination disposent d'un avis de sécurité positif et non périmé, visé à l'article 22*quinquies*/1 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

L'autorité administrative compétente pour le traitement des avis est le ministre de la Justice.

Le Roi définit des mesures de sécurité alternatives à un avis de sécurité, qui sont adaptées aux personnes pour lesquelles un avis de sécurité ne peut être rendu, à défaut d'informations suffisantes les concernant.

Par dérogation à l'alinéa 3, une personne visée à l'alinéa 5 peut faire partie de la Cellule de coordination, en respectant ces mesures de sécurité alternatives et sans disposer d'un avis de sécurité.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut:

1° pour les opérateurs autres que ceux qui disposent déjà d'un officier de sécurité en raison d'autres activités que la Cellule de coordination, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un tel officier en fonction du nombre de demandes reçues de la part des autorités judiciaires, ainsi que les règles qui s'appliquent en l'absence d'un tel officier;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en particulier en matière d'emploi des langues;

3° les règles permettant l'accès des autorités belges habilitées aux coordonnées de la Cellule de coordination et de ses membres.

§ 3. Elke operator stelt een interne procedure vast voor het beantwoorden van de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens van eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.

Elke operator wordt beschouwd als verwerkingsverantwoordelijke in de zin van de AVG, voor de gegevens verwerkt op basis van de artikelen 122, 123, 126, 126/1, 126/2, 126/3 en 127.

§ 4. De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de regels voor de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen. Zo worden onder andere, in voorkomend geval en per betrokken autoriteit, de volgende zaken geregeld:

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de antwoordtermijn;

d) de vereiste beschikbaarheid van de dienst;

e) de nadere regels voor het testen van de samenwerking;

f) de tarieven voor de vergoeding van die samenwerking.

Indien nodig en voor de toepassing van dit artikel, kan de Koning verschillende regels bepalen voor verschillende categorieën van operatoren, met name in functie van het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en of zij al dan niet een elektronischecommunicatienetwerk aanbieden in België.".

Art. 16. In artikel 133, § 1, vijfde lid, van dezelfde wet, gewijzigd bij de wet van 26 november 2021, worden de woorden "de vrije, specifieke en op informatie berustende wilsuiting" vervangen door de woorden "de toestemming in de zin van artikel 4, 11), van de AVG".

Art. 17. In artikel 145 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. Met een geldboete van 50 euro tot 100 000 euro wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 tot 127/3, 133 en de ter uitvoering van de artikelen 9, § 7, 32, 39, § 3, 47, 106/2, 126 tot 126/3, 127, 127/2 en 127/3 genomen besluiten overtreedt.";

2° in de plaats van paragraaf 3*ter*, ingevoegd bij artikel 7 van de wet 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3*ter* ingevoegd:

"§ 3*ter*. Met een geldboete van 50 euro tot 50 000 euro en met een gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in de bepaling onder 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.".

HOOFDSTUK 3. — *Wijziging van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren*

Art. 18. Artikel 8 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, gewijzigd bij de wet van 15 juli 2018, wordt aangevuld met een lid, luidende:

"De ADCC bezorgt na de aanduiding van een kritieke infrastructuur en minstens jaarlijks aan de door de Koning aangewezen dienst de gemeente waarin de kritieke infrastructuur zich bevindt of in voorkomend geval een lijst van gemeenten waarin de kritieke infrastructuren zich bevinden voor de toepassing van artikel 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie.".

§ 3. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs finaux. Il met, sur demande, à la disposition de l'Institut, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur la base des articles 122, 123, 126, 126/1, 126/2, 126/3 et 127.

§ 4. Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles. Sont déterminés, entre autres, les éléments suivants, le cas échéant et par autorité concernée:

a) le mode de transfert, la forme et le contenu des demandes et des réponses;

b) le degré d'urgence de traitement des demandes;

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration.

Si nécessaire et pour l'application du présent article, le Roi peut prévoir des règles différentes pour différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et la fourniture ou non d'un réseau de communications électroniques en Belgique.".

Art. 16. Dans l'article 133, § 1er, alinéa 5, de la même loi, modifié par la loi du 26 novembre 2021, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle" sont remplacés par les mots "le consentement au sens de l'article 4, 11), du RGPD par lequel".

Art. 17. À l'article 145 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021, les modifications suivantes sont apportées:

1° le paragraphe 1er est remplacé par ce qui suit:

"§ 1er. Est punie d'une amende de 50 euros à 100 000 euros, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 à 127/3, 133 et les arrêtés pris en exécution des articles 9, § 7, 32, 39, § 3, 47, 106/2, 126 à 126/3, 127, 127/2 et 127/3.";

2° à la place du paragraphe 3*ter*, inséré par l'article 7 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un paragraphe 3*ter* rédigé comme suit:

"§ 3*ter*. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données conservées par l'opérateur pour les autorités;

2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1°, les détient, les révèle à une autre personne, les divulgue ou en fait un usage quelconque.".

CHAPITRE 3. — *Modification de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques*

Art. 18. L'article 8 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, modifié par la loi du 15 juillet 2018, est complété par un alinéa rédigé comme suit:

"Dans le cadre de l'application de l'article 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, après la désignation d'une infrastructure critique et au moins annuellement, la DGCC fournit au service désigné par le Roi, la commune dans laquelle l'infrastructure critique est située ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées.".

HOOFDSTUK 4. — *Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector*

Art. 19. Artikel 2, eerste lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, gewijzigd bij de wet van 25 april 2007, wordt aangevuld met de bepalingen onder 5° en 6°, luidende:

"5° verzoek om identificatiegegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator of een andere rechtspersoon om andere gegevens te verstrekken dan deze bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie en met het oog op de identificatie van:

— de abonnee of de gewoonlijke gebruiker van de elektronische-communicatiedienst, zijn eindapparatuur of de hardware of software die is ingebouwd in deze eindapparatuur of is geïnstalleerd bij de abonnee met het oog op de verstrekking van de elektronische-communicatiedienst, of;

— de elektronische-communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden;

6° verzoek om metagegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator om andere elektronische-communicatiemetagegevens te verstrekken dan deze bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie en dat geen verzoek om identificatiegegevens is, teneinde met name:

a) de metagegevens in verband met een elektronische communicatie te bepalen;

b) de eindapparatuur te lokaliseren;

c) te bepalen of de eindapparatuur is ingeschakeld of uitgeschakeld.".

Art. 20. In artikel 14, § 1, 3°, van dezelfde wet, vervangen bij de wet van 7 april 2019 en laatstelijk gewijzigd bij de wet van 17 februari 2022, wordt in de bepaling onder d) het cijfer "15" ingevoegd tussen de woorden "de artikelen 14, § 2, 2°," en de woorden "en 21, §§ 5 tot 7".

Art. 21. In dezelfde wet wordt artikel 15, opgeheven bij de wet van 16 maart 2015, hersteld als volgt:

"Art. 15. § 1. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, § 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om identificatiegegevens. Het Instituut bepaalt de termijn waarbinnen de gevraagde gegevens moeten worden meegedeeld.

§ 2. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, § 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om metagegevens. Het Instituut bepaalt de termijn waarbinnen de gevraagde gegevens moeten worden meegedeeld.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid en tenzij anonieme metagegevens worden gevraagd aan de operator, mag het Instituut het verzoek aan de operator pas richten na het voorleggen van een met redenen omkleed en schriftelijk verzoek aan de Gegevensbeschermingsautoriteit en na het ontvangen van de schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid deelt het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dat verzoek, de motivering van het verzoek, alsook de rechtvaardiging van de hoogdringendheid mee aan de Gegevensbeschermingsautoriteit. De Gegevensbeschermingsautoriteit voert daarna een controle uit.

Wanneer na deze latere controle de Gegevensbeschermingsautoriteit weigert de geldigheid te bevestigen van het verzoek dat door het Instituut naar de operator is verstuurd, laat het Instituut dat onverwijld aan de betrokken operator weten en wist het de ontvangen metagegevens.

Voor de toepassing van deze paragraaf vraagt het Instituut aan de operator geanonimiseerde of gepseudonimiseerde metagegevens tenzij, op basis daarvan niet aan het beoogde doel kan worden beantwoord.

CHAPITRE 4. — *Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges*

Art. 19. L'article 2, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, modifié par la loi du 25 avril 2007, est complété par les 5° et 6°, rédigés comme suit:

"5° demande de données d'identification: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur ou à une autre personne morale de communiquer des données autres que celles conservées en vertu des articles 126/1 et 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, et visant à identifier:

— l'abonné ou l'utilisateur habituel du service de communications électroniques, son équipement terminal ou le dispositif matériel ou logiciel intégré dans cet équipement terminal ou installé auprès de l'abonné en vue de la fourniture du service de communications électroniques, ou;

— les services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée;

6° demande de métadonnées: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur de communiquer des métadonnées de communications électroniques autres que celles conservées en vertu des articles 126/1 et 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, autre qu'une demande de données d'identification et visant notamment à:

a) déterminer les métadonnées liées à une communication électronique;

b) localiser l'équipement terminal;

c) déterminer si l'équipement terminal est allumé ou éteint.".

Art. 20. Dans l'article 14, § 1er, 3°, de la même loi, remplacé par la loi du 7 avril 2019 et modifié en dernier lieu par la loi du 17 février 2022, dans le d), le chiffre "15" est inséré entre les mots "les articles 14, § 2, 2°," et les mots "et 21, §§ 5 à 7".

Art. 21. Dans la même loi, l'article 15, abrogé par la loi du 16 mars 2015, est rétabli dans la rédaction suivante:

"Art. 15. § 1er. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, § 1er, 3°, a) et g) à i), l'Institut peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de données d'identification. L'Institut fixe le délai de communication des données demandées.

§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, § 1er, 3°, a) et g) à i), l'Institut peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de métadonnées. L'Institut fixe le délai de communication des données demandées.

Sauf en cas d'urgence dûment justifiée et sauf lorsque des métadonnées anonymes sont demandées à l'opérateur, l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée à l'Autorité de protection des données et après avoir obtenu l'autorisation écrite de cette dernière.

En cas d'urgence dûment justifiée, l'Institut communique à l'Autorité de protection des données, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande ainsi que la justification de l'urgence. L'Autorité de protection des données effectue ultérieurement un contrôle.

Lorsqu'à la suite de ce contrôle ultérieur, l'Autorité de protection des données refuse de confirmer la validité de la demande envoyée par l'Institut à l'opérateur, l'Institut le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

Pour l'application du présent paragraphe, l'Institut demande à l'opérateur des métadonnées anonymisées ou pseudonymisées, sauf lorsqu'elles ne lui permettent pas de rencontrer l'objectif poursuivi.

§ 3. In afwijking van de paragrafen 1 en 2 en om de naleving door een operator van de artikelen 122, 123, 126, 126/1, 126/2, 126/3 of 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie of van een besluit ter uitvoering van een van deze artikelen te controleren, kan het Instituut met een schriftelijk en met redenen omkleed verzoek van een operator eisen om aan het Instituut toegang te verlenen zodat het een databank kan raadplegen die een van deze artikelen of een van deze uitvoeringsbesluiten ten uitvoer legt.

Het eerste lid is wat betreft de artikelen 126, 126/1, 126/2, 126/3 en 127 van de voormelde wet van 13 juni 2005 en de uitvoeringsbesluiten ervan slechts van toepassing voor zover het Instituut op basis van de informatie meegedeeld door de procureur des Konings met toepassing van artikel 21/1, ermee belast wordt de operator te sanctioneren.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de personeelsleden van het Instituut die deze databank mogen raadplegen.

Deze personeelsleden mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 tot 3, moet de motivering van het verzoek gericht aan de operator of aan de Gegevensbeschermingsautoriteit uitgewerkt zijn in het licht van de omstandigheden.

Voor de toepassing van de paragrafen 1 en 2, motiveert het Instituut:

1° het verband tussen de gevraagde gegevens en de aan het Instituut toegewezen opdracht;

2° dat het niet meer gegevens vraagt dan die welke strikt nodig zijn in het kader van die opdracht.

Voor de toepassing van paragraaf 2 geeft het Instituut in het verzoek gericht aan de Gegevensbeschermingsautoriteit het volgende aan:

1° de reden waarom de verstrekking door de operator van geanonimiseerde metagegevens niet volstaat om het nagestreefde doel te bereiken;

2° de reden waarom de verstrekking door de operator van gepseudonimiseerde metagegevens niet volstaat om het nagestreefde doel te bereiken, behalve wanneer het verzoek preciseert dat de operator dergelijke gegevens moet verstrekken.

Worden opgenomen in een inventaris die bij het Instituut wordt bijgehouden:

1° de verzoeken gericht aan de operatoren en aan de Gegevensbeschermingsautoriteit;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de Gegevensbeschermingsautoriteit overeenkomstig paragraaf 2, derde lid;

3° de toestemmingen verleend door de Gegevens-beschermingsautoriteit.".

Art. 22. Artikel 24 van dezelfde wet, vervangen bij de wet van 21 december 2021, waarvan de huidige tekst paragraaf 1 wordt, wordt aangevuld met een paragraaf 2, luidende:

"§ 2. De Koning wijst onder de in paragraaf 1 bedoelde officieren van gerechtelijke politie van het Instituut diegenen aan die belast worden met de controle van de in artikel 25/1, §§ 1 en 3, beoogde verzoeken.

Onverminderd artikel 25, § 5, voeren de officieren van gerechtelijke politie van het Instituut die krachtens het eerste lid door de Koning aangesteld zijn, hun opdracht volledig onafhankelijk uit. Zij mogen niet worden onderworpen aan een ondergeschikt verband ten opzichte van de andere officieren van gerechtelijke politie van het Instituut.".

Art. 23. In artikel 25 van dezelfde wet, gewijzigd bij de wet van 21 december 2021, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie" vervangen door de woorden "officieren van gerechtelijke politie van het Instituut";

2° in paragraaf 3, eerste lid, worden de woorden "personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie" vervangen door de woorden "officieren van gerechtelijke politie van het Instituut";

3° in de paragrafen 4, 5, 6 en 7 worden de woorden "van het Instituut" telkens ingevoegd na de woorden "officieren van gerechtelijke politie".

§ 3. Par dérogation aux paragraphes 1er et 2 et afin de contrôler le respect par un opérateur des articles 122, 123, 126, 126/1, 126/2, 126/3 ou 127 de la loi du 13 juin 2005 relative aux communications électroniques ou d'un arrêté d'exécution d'un de ces articles, l'Institut peut exiger d'un opérateur, par demande écrite et motivée, de fournir l'accès à l'Institut lui permettant de consulter une base de données qui met en œuvre un de ces articles ou un de ces arrêtés d'exécution.

L'alinéa 1er n'est applicable pour ce qui concerne les articles 126, 126/1, 126/2, 126/3 et 127 de la loi précitée du 13 juin 2005 et leurs arrêtés d'exécution que pour autant que l'Institut soit chargé de sanctionner l'opérateur sur la base des informations communiquées par le procureur du Roi en application de l'article 21/1.

La demande adressée à l'opérateur précise les noms des membres du personnel de l'Institut qui peuvent consulter cette base de données.

Ces membres du personnel ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

§ 4. Pour l'application des paragraphes 1er à 3, la motivation de la demande adressée à l'opérateur ou à l'Autorité de protection des données doit être développée au regard des circonstances.

Pour l'application des paragraphes 1er et 2, l'Institut motive:

1° le lien entre les données demandées et la mission attribuée à l'Institut;

2° le caractère strictement nécessaire des données demandées dans le cadre de cette mission.

Pour l'application du paragraphe 2, l'Institut indique dans la demande adressée à l'Autorité de protection des données:

1° le motif pour lequel la communication par l'opérateur de métadonnées anonymisées ne permet pas de rencontrer l'objectif poursuivi;

2° le motif pour lequel la communication par l'opérateur de métadonnées pseudonymisées ne permet pas de rencontrer l'objectif poursuivi, sauf lorsque la demande précise que l'opérateur doit fournir de telles données.

Sont consignées dans un registre tenu auprès de l'Institut:

1° les demandes adressées aux opérateurs et à l'Autorité de protection des données;

2° la motivation de la demande et la justification de l'urgence communiquées à l'Autorité de protection des données conformément au paragraphe 2, alinéa 3;

3° les autorisations données par l'Autorité de protection des données.".

Art. 22. Dans la même loi, l'article 24, remplacé par la loi du 21 décembre 2021, dont le texte actuel formera le paragraphe 1er, est complété par un paragraphe 2 rédigé comme suit:

"§ 2. Le Roi désigne, parmi les officiers de police judiciaire de l'Institut visés au paragraphe 1er, ceux qui sont chargés du contrôle des demandes visées à l'article 25/1, §§ 1er et 3.

Sans préjudice de l'article 25, § 5, les officiers de police judiciaire de l'Institut désignés par le Roi en vertu de l'alinéa 1er, exécutent leur mission en toute indépendance. Ils ne peuvent être soumis à aucun lien de subordination à l'égard des autres officiers de police judiciaire de l'Institut.".

Art. 23. À l'article 25 de la même loi, modifié par la loi du 21 décembre 2021, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 1er, les mots "membres du personnel visés à l'article 24 peuvent, dans l'exercice de leur mission de police judiciaire" sont remplacés par les mots "officiers de police judiciaire de l'Institut peuvent";

2° au paragraphe 3, alinéa 1er, les mots "membres du personnel visés à l'article 24 peuvent, en leur qualité d'officier de police judiciaire" sont remplacés par les mots "officiers de police judiciaire de l'Institut peuvent";

3° aux paragraphes 4, 5, 6 et 7 les mots "de l'Institut" sont chaque fois insérés après les mots "officiers de police judiciaire".

Art. 24. In hoofdstuk III, afdeling 4, onderafdeling 1, van dezelfde wet wordt een artikel 25/1 ingevoegd, luidende:

"Art. 25/1. § 1. Om een inbreuk bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen, kan een officier van gerechtelijke politie van het Instituut, schriftelijk:

1° van een operator eisen om te antwoorden op een verzoek om identificatiegegevens, dat voor deze doeleinden noodzakelijk is;

2° de medewerking vorderen van de personen en instellingen bedoeld in artikel 46quater, § 1, van het Wetboek van strafvordering en van verenigingen die hen vertegenwoordigen, op basis van het kenmerk van de onlinebetaling specifiek voor een elektronische-communicatiedienst die voorafgaandelijk meegedeeld is door een operator overeenkomstig de bepaling onder 1°, om de persoon te identificeren die de dienst heeft betaald;

3° de medewerking vorderen van de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, waar de inschrijving van de abonnee op een elektronische-communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee te identificeren;

4° de medewerking vorderen van alle andere rechtspersonen die abonnee zijn van een operator, of die intekenen in naam en voor rekening van natuurlijke personen op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

Een in het eerste lid bedoeld verzoek mag aan een in het eerste lid bedoelde actor pas worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek gericht aan deze officier overeenkomstig paragraaf 5.

§ 2. Ten behoeve van de vervulling van zijn opdrachten kan een officier van gerechtelijke politie van het Instituut van een operator schriftelijk eisen om te antwoorden op een verzoek om metagegevens, die nodig zijn om een inbreuk bedoeld in artikel 145, § 3, of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid, mag de officier van gerechtelijke politie van het Instituut het verzoek aan de operator pas richten na het voorleggen van een schriftelijk en met redenen omkleed verzoek aan de onderzoeksrechter en na schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dit verzoek, de motivering van het verzoek alsook de rechtvaardiging van de hoogdringendheid mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

Wanneer na deze latere controle de onderzoeksrechter weigert de geldigheid te bevestigen van het verzoek dat door de officier van gerechtelijke politie van het Instituut naar de operator is verstuurd, laat deze officier dat onverwijld aan de betrokken operator weten en wist hij de ontvangen metagegevens.

§ 3. In afwijking van de paragrafen 1 en 2, teneinde de naleving te controleren van de artikelen 126, 126/1, 126/2, 126/3 of 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van de uitvoeringsbesluiten ervan en op schriftelijk en met redenen omkleed verzoek van een officier van gerechtelijke politie van het Instituut, verleent een operator binnen de termijn die vastgesteld is in de vordering toegang zodat zijn databanken die een van deze artikelen of een van deze uitvoeringsbesluiten uitvoeren, geraadpleegd kunnen worden.

Een in het eerste lid bedoeld verzoek mag pas naar een operator worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie van het Instituut. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek overeenkomstig paragraaf 5.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de officieren van gerechtelijke politie van het Instituut die de databank kunnen raadplegen.

Deze officieren mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

Art. 24. Dans le chapitre III, section 4, sous-section 1re, de la même loi, il est inséré un article 25/1, rédigé comme suit:

"Art. 25/1. § 1er. Afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°, un officier de police judiciaire de l'Institut peut, par écrit:

1° exiger d'un opérateur de répondre à une demande de données d'identification qui est nécessaire à ces fins;

2° requérir la collaboration des personnes et institutions visées à l'article 46quater, § 1er, du Code d'instruction criminelle et d'associations les représentant, sur la base de la référence de paiement en ligne spécifique à un service de communications électroniques qui a préalablement été communiquée par un opérateur conformément au 1°, afin d'identifier la personne qui a payé le service;

3° requérir la collaboration des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné;

4° requérir la collaboration de toute autre personne morale qui est l'abonnée d'un opérateur ou qui souscrit à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné ou l'utilisateur habituel du service.

Une demande visée à l'alinéa 1er ne peut être transmise à un acteur visé à l'alinéa 1er qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée adressée à cet officier conformément au paragraphe 5.

§ 2. Pour les besoins de l'accomplissement de ses missions, un officier de police judiciaire de l'Institut peut exiger d'un opérateur, par écrit, de répondre à une demande de métadonnées, qui est nécessaire afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3, ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°.

Sauf en cas d'urgence dûment justifiée, l'officier de police judiciaire de l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée au juge d'instruction et après autorisation écrite de ce dernier.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande et la justification de l'urgence. Un contrôle ultérieur est effectué par le juge d'instruction.

Lorsqu'à la suite de ce contrôle ultérieur, le juge d'instruction refuse de confirmer la validité de la demande envoyée par l'officier de police judiciaire de l'Institut à l'opérateur, cet officier le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 3. Par dérogation aux paragraphes 1er et 2, afin de contrôler le respect des articles 126, 126/1, 126/2, 126/3 ou 127 de la loi du 13 juin 2005 relative aux communications électroniques et de leurs arrêtés d'exécution et à la demande écrite et motivée d'un officier de police judiciaire de l'Institut, un opérateur fournit, dans le délai fixé dans le réquisitoire, un accès permettant de consulter ses bases de données qui mettent en œuvre un de ces articles ou un de ces arrêtés d'exécution.

Une demande visée à l'alinéa 1er ne peut être transmise à un opérateur qu'après autorisation écrite d'un officier de police judiciaire de l'Institut visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée conformément au paragraphe 5.

La demande adressée à l'opérateur précise les noms des officiers de police judiciaire de l'Institut qui peuvent consulter la base de données.

Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

§ 4. Voor de toepassing van de paragrafen 1 en 2, delen de actoren bedoeld in paragraaf 1, eerste lid, aan wie een officier van gerechtelijke politie van het Instituut gegevens gevraagd heeft, de gevraagde gegevens mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

Voor de toepassing van de paragrafen 1 tot 3, is iedere persoon die uit hoofde van zijn functie kennis krijgt van de maatregel of daaraan zijn medewerking verleent, tot geheimhouding verplicht. Iedere schending van de geheimhoudingsplicht wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

Iedere persoon die weigert de raadpleging van de databank mogelijk te maken overeenkomstig paragraaf 3 of die deze raadpleging niet mogelijk maakt binnen de termijn bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

§ 5. Voor de toepassing van de paragrafen 1 tot 3 moet de motivering van het verzoek gericht aan de officier van gerechtelijke politie bedoeld in artikel 24, § 2, of aan de onderzoeksrechter uitgewerkt zijn in het licht van de omstandigheden van het onderzoek.

Voor de toepassing van de paragrafen 1 en 2 vermeldt deze motivering:

1° het verband tussen de gevraagde gegevens en het doel van de opsporing, vaststelling of de vervolging van de specifieke inbreuk dat het verzoek rechtvaardigt;

2° de strikt noodzakelijke aard van de gegevens die worden gevraagd in het kader van het onderzoek.

§ 6. De officieren van gerechtelijke politie van het Instituut nemen op in een inventaris:

1° alle verzoeken bedoeld in de paragrafen 1, 2 en 3;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de onderzoeksrechter overeenkomstig paragraaf 2, derde lid;

3° de in de paragrafen 1, 2 en 3 bedoelde toestemmingen.".

HOOFDSTUK 5. — *Wijzigingen van het Wetboek van strafvordering*

Art. 25. In het Wetboek van strafvordering wordt een artikel 39*quinquies* ingevoegd, luidende:

"Art. 39*quinquies*. § 1. Bij het opsporen van de misdaden en de wanbedrijven kan de procureur des Konings, wanneer er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, bij een met redenen omklede en schriftelijke beslissing aan een of meerdere van de actoren bedoeld in het tweede lid bevelen de gegevens bedoeld in artikel 88*bis*, § 1, eerste lid, die hij noodzakelijk acht en die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Het bevel bedoeld in het eerste lid kan, rechtstreeks of via de door de Koning aangewezen politiedienst, gegeven worden aan:

– de operator van een elektronische communicatienetwerk; en

– iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronische communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De met redenen omklede en schriftelijke beslissing vermeldt:

— de naam van de procureur des Konings die de bewaring beveelt;

— het strafbare feit waarop het bevel betrekking heeft;

— de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen;

— de precieze aanduiding van één of meerdere van de volgende elementen: de persoon of de personen, de communicatiemiddelen of de plaatsen waarop de bewaring betrekking heeft;

§ 4. Pour l'application des paragraphes 1er et 2, les acteurs visés au paragraphe 1er, alinéa 1er, auxquels un officier de police judiciaire de l'Institut a demandé des données, lui communiquent ces données en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire.

Pour l'application des paragraphes 1er à 3, toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

Toute personne qui refuse de permettre la consultation de la base de données conformément au paragraphe 3 ou qui ne permet pas cette consultation dans le délai fixé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

§ 5. Pour l'application des paragraphes 1er à 3, la motivation de la demande adressée à l'officier de police judiciaire visé à l'article 24, § 2, ou au juge d'instruction doit être développée au regard des circonstances de l'enquête.

Pour l'application des paragraphes 1er et 2, cette motivation indique:

1° le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande;

2° le caractère strictement nécessaire des données demandées dans le cadre de l'enquête.

§ 6. Les officiers de police judiciaire de l'Institut consignent dans un registre:

1° l'ensemble des demandes visées aux paragraphes 1er, 2 et 3;

2° la motivation de la demande et la justification de l'urgence communiquées au juge d'instruction conformément au paragraphe 2, alinéa 3;

3° les autorisations prévues aux paragraphes 1er, 2 et 3.".

CHAPITRE 5. — *Modifications du Code d'instruction criminelle*

Art. 25. Dans le Code d'instruction criminelle, il est inséré un article 39*quinquies*, rédigé comme suit:

"Art. 39*quinquies*. § 1er. Lors de la recherche de crimes et délits, le procureur du Roi peut, s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l'alinéa 2, de conserver les données visées à l'article 88*bis*, § 1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.

L'ordre visé à l'alinéa 1er peut être donné, directement ou par l'intermédiaire du service de police désigné par le Roi, à:

– l'opérateur d'un réseau de communications électroniques; et

– toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La décision écrite et motivée mentionne:

— le nom du procureur du Roi qui ordonne la conservation;

— l'infraction qui fait l'objet de l'ordre;

— les circonstances de fait de la cause qui justifient la conservation;

— l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;

— in voorkomend geval, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden;

— de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevel, onverminderd een hernieuwing;

— de duur van bewaring van deze gegevens, die niet langer mag zijn dan zes maanden. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan het bevel tot bewaring mondeling worden gegeven. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde lid.

§ 2. De actoren bedoeld in paragraaf 1, tweede lid, zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

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

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van zesentwintig euro tot twintigduizend euro of met één van die straffen alleen.

§ 4. De toegang tot de overeenkomstig dit artikel bewaarde gegevens is slechts mogelijk met toepassing van artikel 88*bis*.".

Art. 26. In artikel 46*bis* van hetzelfde Wetboek, laatstelijk gewijzigd bij de wet van 25 december 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, kan hij ook, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de personen of instellingen bedoeld in artikel 46quater, § 1, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid;

— de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid;

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, eerste of tweede streepje, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid.";

2° in paragraaf 2 worden het derde en het vierde lid opgeheven;

3° het artikel wordt aangevuld met de paragrafen 3 en 4, luidende:

"§ 3. De actoren bedoeld in paragraaf 1, derde lid, eerste tot derde streepje, van wie de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in paragraaf 1, tweede lid, tweede streepje, gevorderd wordt, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

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

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.".

— le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;

— la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;

— la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.

§ 2. Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

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

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

§ 4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88*bis*.".

Art. 26. À l'article 46*bis* du même Code, modifié en dernier lieu par la loi du 25 décembre 2016, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, un alinéa rédigé comme suit est inséré entre les alinéas 2 et 3:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, il peut également requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:

— des personnes et institutions visées à l'article 46quater, § 1er, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er;

— des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés à l'alinéa 2, premier ou deuxième tiret, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er.";

2° dans le paragraphe 2, les alinéas 3 et 4 sont abrogés;

3° l'article est complété par les paragraphes 3 et 4, rédigés comme suit:

§ 3. Les acteurs visés au paragraphe 1er, alinéa 3, premier à troisième tiret, requis de communiquer l'identification de l'abonné ou de l'utilisateur habituel d'un service visé au paragraphe 1er, alinéa 2, deuxième tiret, communiquent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition.

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

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros.".

Art. 27. In artikel 88*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 1991, vervangen bij de wet van 10 juni 1998 en laatstelijk gewijzigd bij de wet van 5 mei 2019, worden de volgende wijzigingen aangebracht:

1° paragraaf 2, vervangen bij artikel 9 van de wet van 29 mei 2016, zelf vernietigd door arrest n° 57/2021 van het Grondwettelijk Hof, wordt vervangen als volgt:

"§ 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

— voor een strafbaar feit bedoeld in boek II, titel Iter, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan het bevelschrift;

— voor een ander strafbaar feit bedoeld in artikel 90*ter*, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

— voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.";

2° in de plaats van paragraaf 3, ingevoegd bij artikel 9 van de wet van 25 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt de als volgt luidende paragraaf 3 ingevoegd:

"§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

HOOFDSTUK 6. — *Wijziging van de wet van 5 augustus 1992 op het politieambt*

Art. 28. Artikel 42 van de wet van 5 augustus 1992 op het politieambt, gewijzigd bij de wet van 12 november 2017, waarvan de huidige tekst paragraaf 1 zal vormen, wordt aangevuld met de paragrafen 2 en 3, luidende:

"§ 2. Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen.

Enkel de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen en met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, betreffende de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan de opvordering, worden meegedeeld.

De vordering wordt via de officier van gerechtelijke politie bedoeld in het eerste lid, gericht aan:

— de operator van een elektronische communicatienetwerk; of

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronische communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

Art. 27. À l'article 88*bis* du même Code, inséré par la loi du 11 février 1991, remplacé par la loi du 10 juin 1998 et modifié en dernier lieu par la loi du 5 mai 2019, les modifications suivantes sont apportées:

1° le paragraphe 2, remplacé par l'article 9 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, est remplacé par ce qui suit:

"§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base des articles 126/1 et 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent:

— pour une infraction visée au livre II, titre Iter, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;

— pour une autre infraction visée à l'article 90*ter*, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;

— pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.";

2° à la place du paragraphe 3, inséré par l'article 9 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un paragraphe 3 rédigé comme suit:

"§ 3. La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

CHAPITRE 6. — *Modification de la loi du 5 août 1992 sur la fonction de police*

Art. 28. L'article 42 de la loi du 5 août 1992 sur la fonction de police, modifié par la loi du 12 novembre 2017, dont le texte actuel formera le paragraphe 1er, est complété par les paragraphes 2 et 3, rédigés comme suit:

"§ 2. Un officier de police judiciaire de la Cellule Personnes disparues de la police fédérale peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue.

Seules les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication et relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, concernant la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données, sont communiquées.

La réquisition est adressée par l'officier de police judiciaire visé à l'alinéa 1er, à:

— l'opérateur d'un réseau de communications électroniques; ou

— toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

§ 3. De Cel Vermiste Personen stelt het Controleorgaan uiterlijk binnen 48 uur na de vordering in kennis van de vordering en de motivering ervan.

Indien het Controleorgaan van oordeel is dat niet aan de voorwaarden voor de uitvoering van deze vordering is voldaan, beveelt zij, met opgave van redenen, dat de aldus verkregen gegevens niet mogen worden gebruikt en vernietigd moeten worden.

Deze met redenen omklede beslissing wordt door het Controleorgaan zo spoedig mogelijk meegedeeld aan de Cel Vermiste Personen.".

HOOFDSTUK 7. — *Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*

Art. 29. In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, laatstelijk gewijzigd bij de wet van 30 maart 2017, wordt de bepaling onder 10° aangevuld met de woorden ", ongeacht de aard van de afzender of de ontvanger".

Art. 30. In de inleidende zin van artikel 7 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 april 2016, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Veiligheid van de Staat" en "heeft als opdracht".

Art. 31. In artikel 11, § 1, van dezelfde wet, laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Inlichting en Veiligheid" en "heeft als opdracht".

Art. 32. In hoofdstuk III van dezelfde wet wordt een afdeling 3/1 ingevoegd, luidende "Vorderingen tot bewaring".

Art. 33. In afdeling 3/1, ingevoegd bij artikel 32, wordt een artikel 13/6 ingevoegd, luidende:

"Art. 13/6. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst om over te gaan tot:

1° de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering;

2° de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt.

De in het eerste lid bedoelde vordering is gebaseerd op een schriftelijke en met redenen omklede beslissing van het diensthoofd of zijn gedelegeerde.

§ 2. De in paragraaf 1, eerste lid, bedoelde vordering vermeldt:

1° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

2° de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden;

3° voor de maatregel bedoeld in paragraaf 1, eerste lid, 1°, de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

4° voor de maatregel bedoeld in paragraaf 1, eerste lid, 2°:

— de duur van de maatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

— de bewaartermijn van gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

5° de datum van de vordering;

6° de handtekening van het diensthoofd of van zijn gedelegeerde.

§ 3. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de bewaring mondeling vorderen. Deze mondelinge vordering wordt schriftelijk bevestigd uiterlijk op de eerstvolgende werkdag.

§ 4. De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.

Elke beslissing tot vordering en de motivering ervan worden ter kennis gebracht van het Vast Comité I. Indien het Vast Comité I een onwettigheid vaststelt, maakt het een einde aan de vordering.

§ 3. La réquisition et sa justification sont notifiées par la Cellule Personnes disparues à l'Organe de contrôle, au plus tard dans les 48 heures après la réquisition.

Si l'Organe de contrôle estime que les conditions pour effectuer cette réquisition ne sont pas remplies, il ordonne, de manière motivée, l'interdiction d'exploiter les données obtenues par ce moyen et l'effacement des données.

Cette décision motivée est notifiée dans les meilleurs délais possibles par l'Organe de contrôle à la Cellule Personnes disparues.".

CHAPITRE 7. — *Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Art. 29. Dans l'article 3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, modifié en dernier lieu par la loi du 30 mars 2017, le 10° est complété par les mots ", quelle que soit la nature de l'émetteur ou du récepteur".

Art. 30. Dans la phrase introductive de l'article 7 de la même loi, modifié en dernier lieu par la loi du 21 avril 2016, les mots ", chargée de la sécurité nationale," sont insérés entre les mots "La Sûreté de l'État" et "a pour mission".

Art. 31. Dans l'article 11, § 1er, de la même loi, modifié en dernier lieu par la loi du 30 mars 2017, les mots ", chargé de la sécurité nationale," sont insérés entre les mots "Renseignement et de la Sécurité" et "a pour mission".

Art. 32. Au chapitre III de la même loi, une section 3/1 est insérée, intitulée "Réquisitions de conservation".

Art. 33. Dans la section 3/1, insérée par l'article 32, il est inséré un article 13/6, rédigé comme suit:

"Art. 13/6. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à:

1° la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition;

2° la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.

La réquisition visée à l'alinéa 1er repose sur une décision écrite et motivée du dirigeant du service ou de son délégué.

§ 2. La réquisition visée au paragraphe 1er, alinéa 1er, mentionne:

1° la nature des données de trafic et de localisation à conserver;

2° les personnes, les groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées;

3° pour la mesure visée au paragraphe 1er, alinéa 1er, 1°, le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

4° pour la mesure visée au paragraphe 1er, alinéa 1er, 2°:

— la durée de la mesure, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

— le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication, sans préjudice de la possibilité de prolongation en suivant la même procédure;

5° la date de la réquisition;

6° la signature du dirigeant du service ou de son délégué.

§ 3. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir la conservation verbalement. Cette réquisition verbale est confirmée par écrit au plus tard le premier jour ouvrable qui suit.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.

Chaque décision de réquisition est notifiée avec sa motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.

Indien de vordering voortijdig wordt beëindigd, wordt de gevorderde operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 5. Voor de uitvoering van de vordering kan het diensthoofd of zijn gedelegeerde de medewerking vorderen van het Instituut bedoeld in artikel 2, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag.

§ 6. Eenieder die weigert zijn medewerking te verlenen aan de in de paragrafen 1 en 5 bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

§ 7. De Koning kan, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie, de nadere regels bepalen voor de samenwerking van de operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst.".

Art. 34. In dezelfde afdeling wordt een artikel 13/7 ingevoegd, luidende:

"Art. 13/7. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, de medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronische communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen.

§ 2. De in paragraaf 1 bedoelde vordering kan enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de commissie. De commissie geeft haar akkoord binnen vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

§ 3. De vraag van het diensthoofd om een vordering tot bewaring in te stellen vermeldt, op straffe van onwettigheid:

1° de ernstige dreiging tegen de nationale veiligheid die reëel en actueel of voorzienbaar is;

2° de feitelijke omstandigheden die de ongedifferentieerde en algemene bewaring van de verkeers- en lokalisatiegegevens rechtvaardigen;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de bewaringsmaatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering. Hij kan volgens dezelfde procedure worden verlengd;

5° de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie. Hij kan volgens dezelfde procedure worden verlengd;

6° in voorkomend geval, de redenen die de in paragraaf 5 bedoelde hoogdringendheid rechtvaardigen;

7° de datum van de vraag;

8° de handtekening van het diensthoofd.

§ 4. De in paragraaf 1 bedoelde vordering vermeldt:

1° de datum van het akkoord van de commissie;

2° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

3° de duur van de maatregel en de bewaartermijn van de gegevens;

4° de datum van de vordering;

5° de handtekening van het diensthoofd of zijn gedelegeerde.

§ 5. In geval van hoogdringendheid vraagt het diensthoofd vooraf om het mondelinge akkoord van de voorzitter van de commissie of, indien deze niet beschikbaar is, een ander lid van de commissie. De auteur van het akkoord informeert onmiddellijk de andere commissieleden. Het diensthoofd bevestigt zijn vraag schriftelijk binnen vierentwintig uur volgend op het akkoord. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord is gedurende vijf dagen geldig.

§ 6. De vordering tot een algemene en ongedifferentieerde bewaring wordt bevestigd bij koninklijk besluit.

Het koninklijk besluit vermeldt enkel:

1° de datum van het akkoord van de commissie;

2° de datum van de vordering;

Lorsqu'il est mis fin prématurément à la réquisition, l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques requis en est averti le plus rapidement possible.

§ 5. Pour l'exécution de la réquisition, le dirigeant du service ou son délégué peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale.

§ 6. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 5 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 7. Le Roi peut déterminer, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques.".

Art. 34. Dans la même section, il est inséré un article 13/7, rédigé comme suit:

"Art. 13/7. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques afin de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux.

§ 2. La réquisition visée au paragraphe 1er ne peut avoir lieu qu'avec l'accord écrit préalable de la commission. La commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

§ 3. La demande du dirigeant du service de requérir la conservation mentionne, sous peine d'illégalité:

1° la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible;

2° les circonstances de fait qui justifient la conservation généralisée et indifférenciée des données de trafic et de localisation;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure de conservation, qui ne peut excéder six mois à compter de la date de la réquisition. Elle peut être prolongée en suivant la même procédure;

5° le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication. Il peut être prolongé en suivant la même procédure;

6° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 5;

7° la date de la demande;

8° la signature du dirigeant du service.

§ 4. La réquisition visée au paragraphe 1er mentionne:

1° la date de l'accord de la commission;

2° la nature des données de trafic et de localisation à conserver;

3° la durée de la mesure et le délai de conservation des données;

4° la date de la réquisition;

5° la signature du dirigeant du service ou de son délégué.

§ 5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la commission ou, en cas d'indisponibilité, d'un autre membre de la commission. L'auteur de l'accord en informe immédiatement les autres membres de la commission. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant l'accord. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§ 6. La réquisition de conservation généralisée et indifférenciée est confirmée par arrêté royal.

L'arrêté royal ne mentionne que:

1° la date de l'accord de la commission;

2° la date de la réquisition;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de maatregel en de bewaartermijn van de gegevens.

Bij gebrek aan bevestiging bij koninklijk besluit binnen een maand na de vordering, eindigt deze vordering.

De gevorderde operatoren van een elektronisch communicatienetwerk en verstrekkers van een elektronische communicatiedienst worden hiervan zo spoedig mogelijk op de hoogte gebracht.

§ 7. Voor de uitvoering van de vordering kan het diensthoofd de medewerking vorderen van het Instituut bedoeld in artikel 2, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag en het akkoord van de commissie.

§ 8. Eenieder die weigert zijn medewerking te verlenen aan de in de paragrafen 1 en 7 bedoelde vorderingen wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

§ 9. De commissie geeft onverwijld de vraag van het diensthoofd en haar akkoord door aan het Vast Comité I.

§ 10. De inlichtingen- en veiligheidsdienst brengt om de twee weken verslag uit aan de commissie over de evolutie van de dreiging. Dit verslag belicht de elementen die ofwel de handhaving van de algemene en ongedifferentieerde bewaring, ofwel de beëindiging ervan, rechtvaardigen.

§ 11. Het diensthoofd beëindigt de vordering, niettegenstaande de bevestiging bij koninklijk besluit, wanneer de bewaring niet langer van nut is voor de bestrijding van de reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, wanneer deze dreiging is verdwenen of wanneer hij een onwettigheid vaststelt.

Wanneer de commissie of het Vast Comité I een onwettigheid vaststelt, wordt een einde gemaakt aan de vordering niettegenstaande de bevestiging bij koninklijk besluit.

Indien de vordering voortijdig wordt beëindigd, worden de gevorderde operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 12. De Koning bepaalt, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie, de nadere regels voor de samenwerking van de operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst.".

Art. 35. In artikel 16/2, § 2, van dezelfde wet, ingevoegd bij de wet van 1 september 2016, worden de volgende wijzigingen aangebracht:

a) het eerste lid wordt vervangen als volgt:

"De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst, de medewerking vorderen van:

1° de personen of instellingen bedoeld in artikel 5, § 1, eerste lid, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten en van de personen of instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een operator of verstrekker met toepassing van paragraaf 1;

2° andere rechtspersonen die de abonnee zijn van een operator of verstrekker zoals bedoeld in paragraaf 1 of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een operator of verstrekker in toepassing van paragraaf 1.";

b) in het derde lid worden de woorden "Iedere bank en iedere financiële instelling" vervangen door de woorden "Iedere persoon en iedere instelling".

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure et le délai de conservation des données.

En l'absence de confirmation par arrêté royal dans le mois de la réquisition, cette réquisition prend fin.

Les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 7. Pour l'exécution de la réquisition, le dirigeant du service peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale et l'accord de la commission.

§ 8. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 7 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 9. La commission transmet sans délai la demande du dirigeant du service et son accord au Comité permanent R.

§ 10. Le service de renseignement et de sécurité fait rapport à la commission toutes les deux semaines sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

§ 11. Le dirigeant du service met fin à la réquisition, nonobstant la confirmation par arrêté royal, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, lorsque cette menace a disparu ou lorsqu'il constate une illégalité.

Lorsque la commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.

Lorsqu'il est mis fin prématurément à la réquisition, les opérateurs d'un réseau de communications électroniques ou les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 12. Le Roi détermine, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques.".

Art. 35. À l'article 16/2, § 2, de la même loi, inséré par la loi du 1er septembre 2016, les modifications suivantes sont apportées:

a) l'alinéa 1er est remplacé par ce qui suit:

"Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques, requérir le concours:

1° des personnes ou institutions visées à l'article 5, § 1er, alinéa 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces et des personnes ou institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec les valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er;

2° des autres personnes morales qui sont l'abonné d'un opérateur ou d'un fournisseur visés au paragraphe 1er ou qui souscrivent au nom et pour le compte de personnes physiques à un service de communications électroniques, sur la base des données qui ont été préalablement communiquées par un opérateur ou un fournisseur en application du paragraphe 1er.";

b) dans l'alinéa 3, les mots "Toute banque et toute institution financière" sont remplacés par les mots "Toute personne et toute institution".

Art. 36. In artikel 18/7 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wetten van 5 februari 2016 en 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in de inleidende zin van paragraaf 1 worden de woorden "In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, "vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,";

2° in paragraaf 1 worden in de bepaling onder 2° de woorden "de mededeling van de facturen met betrekking tot de geïdentificeerde abonnementen," ingevoegd tussen de woorden "tot het bekomen van" en de woorden "de gegevens betreffende de betalingswijze";

3° in paragraaf 3, tweede lid, worden de woorden "het diensthoofd" vervangen door de woorden "de betrokken dienst".

Art. 37. Artikel 18/8 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij artikel 14 van de wet van 29 mei 2016, zelf vernietigd bij het arrest nr. 57/2021 van het Grondwettelijk Hof, en bij de wet van 30 maart 2017, wordt vervangen als volgt:

"Art. 18/8. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.

In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.

De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.

§ 2. [...]

§ 3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie.

Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.

§ 4. [...]".

Art. 38. In artikel 18/14, § 1, eerste lid, van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, worden de woorden "In het belang van de uitoefening van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten" vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,".

Art. 39. In artikel 18/17, § 1, van dezelfde wet ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, worden de woorden "In het belang van de uitvoering van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten", vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,".

HOOFDSTUK 8. — *Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten*

Art. 40. In artikel 81 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, hersteld bij de wet van 2 mei 2007 en gewijzigd bij de wetten van 25 april 2014 en 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden in het derde lid de woorden "bedoeld in het eerste lid" ingevoegd tussen de woorden "in zijn beslissing" en de woorden "opgave van";

Art. 36. À l'article 18/7 de la même loi, inséré par la loi du 4 février 2010 et modifié par les lois des 5 février 2016 et 30 mars 2017, les modifications suivantes sont apportées:

1° dans la phrase introductive du paragraphe 1er, les mots "Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions";

2° dans le paragraphe 1er, 2°, les mots "la communication des factures afférentes aux abonnements identifiés," sont insérés entre les mots "afin d'obtenir" et les mots "les données relatives à la méthode de paiement";

3° dans le paragraphe 3, alinéa 2, les mots "le dirigeant du service" sont remplacés par les mots "le service concerné".

Art. 37. L'article 18/8 de la même loi, inséré par la loi du 4 février 2010 et modifié par l'article 14 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, et par la loi du 30 mars 2017, est remplacé par ce qui suit:

"Art. 18/8. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques, procéder ou faire procéder:

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

2° à la localisation de l'origine ou de la destination de communications électroniques.

Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.

La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.

§ 2. [...]

§ 3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au paragraphe 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions.

Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à vingt mille euros.

§ 4. [...]".

Art. 38. Dans l'article 18/14, § 1er, alinéa 1er, de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les mots "Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions,".

Art. 39. À l'article 18/17, § 1er, de la même loi inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les mots "Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions,".

CHAPITRE 8. — *Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers*

Art. 40. À l'article 81 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, rétabli par la loi du 2 mai 2007 et modifié par les lois des 25 avril 2014 et 31 juillet 2017, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, alinéa 3, les mots "visée à l'alinéa 1er" sont insérés entre les mots "dans sa décision" et les mots "les circonstances de fait";

2° paragraaf 1 wordt aangevuld met een lid, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een in het tweede lid, 2°, bedoelde dienst, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, ook de medewerking vorderen van:

— de personen of instellingen bedoeld in artikel 5, § 1, eerste lid, 3° tot 22°, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— de gesloten centra of woonunits bedoeld in de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid.";

3° in paragraaf 2, tweede lid, worden de woorden "de in het eerste lid bedoelde actoren" vervangen door de woorden "de actoren bedoeld in paragraaf 1, tweede lid, en de personen en instellingen bedoeld in paragraaf 1, vierde lid,".

Art. 41. In artikel 84 van dezelfde wet, hersteld bij de wet van 2 mei 2007 en gewijzigd bij de wetten van 25 april 2014 en 31 juli 2017, wordt een paragraaf 1*bis*/1 ingevoegd, luidende:

"§ 1*bis*/1. Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen om de mededeling van deze gegevens te vorderen.

Paragrafen 1, vierde en vijfde lid, en 3, zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.

De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, verzoekt onverwijld de voorafgaande toestemming van een onderzoeksrechter om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens die het voorwerp uitmaken van een in het eerste lid bedoeld bevel tot bewaring en bezorgt dit bevel aan de onderzoeksrechter. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel tot bewaring betrekking heeft of oordeelt dat dit bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel. In dat geval brengt de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de bestemmeling van het bevel tot bewaring er onverwijld van op de hoogte dat het vervallen is.".

HOOFDSTUK 9. — *Wijzigingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk-en informatiesystemen van algemeen belang voor de openbare veiligheid*

Art. 42. Artikel 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt vervangen als volgt:

"Art. 62. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

2° le paragraphe 1er est complété par un alinéa, rédigé comme suit:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, 2°, l'auditeur ou, en son absence, l'auditeur adjoint peut également requérir la collaboration:

— des personnes et institutions visées à l'article 5, § 1er, alinéa 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er;

— des centres fermés ou des lieux d'hébergement visés aux articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectuée, et qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'aliéa 1er;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés à l'alinéa 2, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er.";

3° dans le paragraphe 2, alinéa 2, les mots "les acteurs visés à l'alinéa 1er" sont remplacés par les mots "les acteurs visés au paragraphe 1er, alinéa 2, ainsi que les personnes et institutions visées au paragraphe 1er, alinéa 4,".

Art. 41. Dans l'article 84 de la même loi, rétabli par la loi du 2 mai 2007 et modifié par les lois des 25 avril 2014 et 31 juillet 2017, il est inséré un paragraphe 1er*bis*/1 rédigé comme suit:

"§ 1er*bis*/1. Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

Les paragraphes 1er, alinéas 4 et 5, et 3, s'appliquent par analogie à l'ordre visé à l'alinéa 1er.

Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soient garanties et à ce que les données soient conservées de manière sécurisée.

L'auditeur ou, en son absence, l'auditeur adjoint demande sans délai l'autorisation préalable d'un juge d'instruction pour requérir la communication des données visées au paragraphe 1er, alinéa 1er, qui font l'objet d'un ordre de conservation visé à l'alinéa 1er, et fait part de cet ordre au juge d'instruction. Lorsque le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre de conservation ou s'il estime que cet ordre n'était pas légitime ou justifié, cet ordre devient caduc. Dans ce cas, l'auditeur ou, en son absence, l'auditeur adjoint fait sans délai savoir au destinataire de l'ordre de conservation que celui-ci est devenu caduc.".

CHAPITRE 9. — *Modifications de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*

Art. 42. L'article 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est remplacé par ce qui suit:

"Art. 62. § 1er. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, eerste lid, a) tot e), kan het nationale CSIRT identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 betreffende de elektronische communicatie verkrijgen van een operator als bedoeld in artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.

De doeleinden van voornoemde taken zijn:

— het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

— het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen;

— het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.

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

Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 betreffende de elektronische communicatie die geen in het derde lid bedoelde gegevens zijn, stuurt, wordt dat verzoek vooraf gecontroleerd door de Gegevensbeschermingsautoriteit.

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

Indien de Gegevensbeschermingsautoriteit, na de in het vijfde lid bedoelde controle, weigert de geldigheid van het in het vierde lid bedoelde verzoek om elektronische-communicatiemetagegevens te bevestigen, stelt het nationale CSIRT de betrokken operator daarvan onverwijld in kennis en verwijdert het de ontvangen metagegevens.

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

Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.

§ 3. Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid, waarbij er steeds bij voorrang voor wordt gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.".

Art. 43. In artikel 65, § 2, van dezelfde wet worden de woorden "elektronische communicatiegegevens," ingevoegd tussen de woorden "verbindingsgegevens of -identificatoren," en de woorden "locatiegegevens".

HOOFDSTUK 10. — *Wijziging van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de verbruikers op het stuk van de voedingsmiddelen en andere produkten*

Art. 44. Artikel 11, § 1, van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de verbruikers op het stuk van de voedingsmiddelen en andere produkten, vervangen bij de wet van 10 april 2014, wordt aangevuld met vier leden, luidende:

"Zij mogen natuurlijke en rechtspersonen identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, alinéa 1er, a) à e), le CSIRT national peut obtenir d'un opérateur visé à l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données d'identification visées à l'article 2, alinéa 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.

Les finalités poursuivies par les tâches précitées sont:

— la prévention de menaces graves contre la sécurité publique;

— l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information;

— la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave.

Lorsque le CSIRT national adresse à un opérateur une demande de données d'identification visées à l'article 2, alinéa 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi du 13 juin 2005 relative aux communications électroniques autres que celles visées à l'alinéa 3, cette demande fait l'objet d'un contrôle préalable par l'Autorité de protection des données.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 4 et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 4 pour permettre un contrôle ultérieur.

Lorsqu'à la suite du contrôle visé à l'alinéa 5, l'Autorité de protection des données refuse de confirmer la validité de la demande de métadonnées de communications électroniques visée à l'alinéa 4, le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

Le directeur du CSIRT national désigne expressément les personnes habilitées à traiter ces données de communications électroniques.

Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.

§ 3. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 4. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.".

Art. 43. Dans l'article 65, § 2, de la même loi, les mots "des données de communications électroniques," sont insérés entre les mots "des données ou des identifiants de connexion," et les mots "des données de géolocalisation".

CHAPITRE 10. — *Modification de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits*

Art. 44. L'article 11, § 1er, de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits, remplacé par la loi du 10 avril 2014, est complété par quatre alinéas rédigés comme suit:

"Ils peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique.

Hiertoe mogen zij op met redenen omkleed verzoek de verstrekking van de identificatiedocumenten en -gegevens vorderen van:

1° de operator van een elektronische-communicatienetwerk; en

2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische-communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronische-communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische-communicatiedienst begrepen.

Onverminderd een eventuele delegatie, dient elk identificatieverzoek voorafgaandelijk door het diensthoofd van de Inspectiedienst Consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.

Met het oog op de identificatie van de betrokkene kan het diensthoofd van de Inspectiedienst Consumptieproducten de medewerking vorderen van de personen of instellingen bedoeld in artikel 5, § 1, eerste lid, 3° tot 22°, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een operator in de zin van artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.".

HOOFDSTUK 11. — *Overgangsbepalingen*

Art. 45. De gerichte gegevensbewaring op basis van de criteria bedoeld in artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 betreffende de elektronische communicatie treedt in werking op de door de Koning bij een besluit vastgesteld na overleg in de Ministerraad bepaalde datum en uiterlijk op 1 januari 2027.

Bij de eerste toepassing van artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 betreffende de elektronische communicatie, maken de in artikel 126/3, § 6, tweede lid, van dezelfde wet bedoelde bevoegde autoriteiten de nodige informatie over aan de de door de Koning aangewezen dienst op een datum die vastgesteld wordt bij het in het eerste lid bedoelde koninklijk besluit en uiterlijk op 1 januari 2026.

Art. 46. De ministers van Justitie en van Binnenlandse Zaken bepalen de bewaartermijn van de gegevens bedoeld in artikel 126/2, § 2, van de wet van 13 juni 2005 betreffende de elektronische communicatie, per gerechtelijk arrondissement en per politiezone, en op basis van de criteria bedoeld in artikel 126/3, § 1, van dezelfde wet, die zal gelden vanaf de inwerkingtreding van deze wet tot de publicatie van het ministerieel besluit bedoeld in artikel 126/3, § 1, tiende lid, van dezelfde wet.

Art. 47. Uiterlijk op de eerste dag die volgt op de afloop van een termijn van twee jaar die ingaat op de dag waarop deze wet wordt bekendgemaakt in het *Belgisch Staatsblad*, bewaren de operatoren de volgende gegevens:

1° het MAC-adres, "*Media Access Control address*", bedoeld in de artikelen 126, § 1, eerste lid, 16°, derde streepje, en 126/2, § 2, 2°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

2° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt tijdens de communicatie, waarvan sprake in artikel 126/2, § 2, eerste lid, 6°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

3° de gegevens bedoeld in artikel 126/2, § 2, 8° en 9°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Art. 48. De wijzigingen van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, vervangen bij artikel 12, zijn enkel van toepassing voor de identificaties door de operatoren van de abonnees die gebeuren na de inwerkingtreding van deze wet.

Artikel 127, § 6, tweede lid, van de voormelde wet van 13 juni 2005 wordt van kracht twee jaar na de bekendmaking van deze wet.

Tussen de inwerkingtreding van deze wet en de in het tweede lid vastgestelde datum maken de in artikel 127, § 6, tweede lid, van de voormelde wet van 13 juni 2005 bedoelde operatoren het voor de abonnees mogelijk om zich te identificeren aan de hand van de documenten bedoeld in artikel 127, § 6, eerste lid, 1° tot 18°, 20° tot 24°, 26°, 28°, en 31°, van diezelfde wet, in het kader van minstens één identificatiemethode van hun keuze.

De operatoren leggen artikel 127, § 7, van de voormelde wet van 13 juni 2005 uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer.

À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification à:

1° l'opérateur d'un réseau de communications électroniques; et

2° toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Sans préjudice d'une éventuelle délégation, chaque demande d'identification doit être approuvée au préalable, par écrit, par le chef du service Inspection Produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement.

Pour procéder à l'identification de la personne concernée, le chef du service Inspection Produits de consommation peut requérir la collaboration des personnes ou institutions visées à l'article 5, § 1er, alinéa 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un opérateur au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques.".

CHAPITRE 11. — *Dispositions transitoires*

Art. 45. La conservation ciblée des données sur la base des critères visés à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, entre en vigueur à la date fixée par le Roi par arrêté délibéré en Conseil des ministres, et au plus tard le 1er janvier 2027.

Pour la première application de l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, les autorités compétentes visées à l'article 126/3, § 6, alinéa 2, de la même loi, transmettent les informations nécessaires au service désigné par le Roi à une date fixée par l'arrêté royal visé à l'alinéa 1er et au plus tard le 1er janvier 2026.

Art. 46. Les ministres de la Justice et de l'Intérieur déterminent la durée de conservation des données visées à l'article 126/2, § 2, de la loi du 13 juin 2005 relative aux communications électroniques, par arrondissement judiciaire et par zone de police, et sur la base des critères visés à l'article 126/3, § 1er, de la même loi, qui s'applique à partir de l'entrée en vigueur de la présente loi jusqu'à la publication de l'arrêté ministériel visé à l'article 126/3, § 1er, alinéa 10, de la même loi.

Art. 47. Les opérateurs conservent les données suivantes au plus tard le premier jour qui suit l'expiration d'un délai de deux ans prenant cours le jour de la publication de la présente loi au *Moniteur belge*:

1° l'adresse MAC, "Media Access Control address", visée aux articles 126, § 1er, alinéa 1er, 16°, troisième tiret, et 126/2, § 2, 2°, de la loi du 13 juin 2005 relative aux communications électroniques;

2° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisées au cours de la communication, visées à l'article 126/2, § 2, alinéa 1er, 6°, de la loi du 13 juin 2005 relative aux communications électroniques;

3° les données visées à l'article 126/2, § 2, 8° et 9°, de la loi du 13 juin 2005 relative aux communications électroniques.

Art. 48. Les modifications à l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, remplacé par l'article 12, ne s'appliquent que pour les identifications par les opérateurs des abonnés qui sont réalisées après l'entrée en vigueur de la présente loi.

L'article 127, § 6, alinéa 2, de la loi précitée du 13 juin 2005 entre en vigueur deux ans après la publication de la présente loi.

Entre l'entrée en vigueur de la présente loi et la date fixée à l'alinéa 2, les opérateurs visés à l'article 127, § 6, alinéa 2, de la loi précitée du 13 juin 2005 permettent aux abonnés de s'identifier à l'aide des documents visés à l'article 127, § 6, alinéa 1er, 1° à 18°, 20° à 24°, 26°, 28°, et 31°, de cette même loi, dans le cadre d'au moins une méthode d'identification de leur choix.

Les opérateurs mettent en œuvre l'article 127, § 7, de la loi précitée du 13 juin 2005 au plus tard 24 mois après la publication de la présente loi.

Wanneer een operator de indirecte identificatiemethode bedoeld in artikel 127, § 10, eerste lid, 3°, van de voormelde wet van 13 juni 2005 ten uitvoer legt, bewaart hij de gegevens die erin worden beoogd uiterlijk 24 maanden na de bekendmaking van deze wet.

De operatoren leggen artikel 127, § 10, eerste lid, 6°, en tweede lid, van de voormelde wet van 13 juni 2005 uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer. De in deze bepalingen bedoelde rechtspersonen verkrijgen de erkenning uiterlijk 24 maanden na de bekendmaking van deze wet.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 20 juli 2022.

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister van Financiën,
belast met de Coördinatie van de fraude bestrijding,
V. VAN PETEGHEM

De Minister van Volksgezondheid,
F. VANDENBROUCKE

De Minister van Telecommunicatie,
P. DE SUTTER

De Minister van Justitie,
V. VAN QUICKENBORNE

De Minister van Defensie,
L. DEDONDER

De Minister Van Binnenlandse Zaken,
A. VERLINDEN

De Staatssecretaris voor Digitalisering,
belast met Privacy,
M. MICHEL

Met 's Lands zegel gezegeld:

De Minister van Justitie,

V. VAN QUICKENBORNE

Nota

(1) Kamer van volksvertegenwoordigers
(www.dekamer.be)
Stukken : 55 - 2572
Integraal Verslag : 7 juli 2022

Lorsqu'un opérateur met en œuvre la méthode d'identification indirecte visée à l'article 127, § 10, alinéa 1er, 3°, de la loi précitée du 13 juin 2005, il conserve les données qui y sont visées au plus tard 24 mois après la publication de la présente loi.

Les opérateurs mettent en œuvre l'article 127, § 10, alinéa 1er, 6°, et alinéa 2, de la loi précitée du 13 juin 2005 au plus tard 24 mois après la publication de la présente loi. Les personnes morales visées par ces dispositions obtiennent l'agrément au plus tard 24 mois après la publication de la présente loi.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'Etat et publiée par le *Moniteur belge.*

Donné à Bruxelles, le 20 juillet 2022.

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

Le Ministre des Finances,
chargé de la Coordination de la lutte contre la fraude,
V. VAN PETEGHEM

Le Ministre de la Santé publique,
F. VANDENBROUCKE

La Ministre des Télécommunications,
P. DE SUTTER

Le Ministre de la Justice,
V. VAN QUICKENBORNE

La Ministre de la Défense,
L. DEDONDER

La Ministre de l'Intérieur,
A. VERLINDEN

Le Secrétaire d'État à la Digitalisation,
chargé de la Protection de la vie privée,
M. MICHEL

Scellé du sceau de l'Etat :

Le Ministre de la Justice,

V. VAN QUICKENBORNE

Note

(1) Chambre des représentants
(www.lachambre.be)
Documents : 55 - 2572
Compte rendu intégral : 7 juillet 2022

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2022/15553]

30 JULI 2022. — Wet om justitie menselijker, sneller en straffer te maken II (1)

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK 1. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2. — *Wijziging van het Wetboek van strafvordering*

Art. 2. In het Wetboek van strafvordering wordt een artikel 258/1 ingevoegd, luidende:

"Art. 258/1. § 1. De voorzitter kan beslissen, in het belang van een goede rechtsbedeling, hetzij door de onevenredigheid tussen de fysieke onthaalcapaciteit van het hof van assisen en het aantal procespartijen, hetzij door het groot aantal slachtoffers met een woonplaats in het buitenland, dat het verloop van de terechtzitting het voorwerp zal uitmaken van een geluidsopname of van een audiovisuele opname die de uitgestelde uitzending ervan mogelijk maakt, door middel van een

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2022/15553]

30 JUILLET 2022. — Loi visant à rendre la justice plus humaine, plus rapide et plus ferme II (1)

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

CHAPITRE 1er. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2. — *Modifications du Code d'instruction criminelle*

Art. 2. Dans le Code d'instruction criminelle, il est inséré un article 258/1 rédigé comme suit :

"Art. 258/1. § 1er. Le président peut décider, dans l'intérêt de la bonne administration de la justice, en raison soit de la disproportion entre la capacité d'accueil physique de la cour d'assises et le nombre de parties au procès, soit du grand nombre de victimes avec un domicile à l'étranger, que le déroulement de l'audience fera l'objet d'une captation sonore ou audiovisuelle permettant sa diffusion en différé, par un moyen de télécommunication garantissant la confidentialité de