

ROYAUME DE BELGIQUE	KONINKRIJK BELGIE
_____	_____
SERVICE PUBLIC FEDERAL JUSTICE SERVICE PUBLIC FEDERAL DEFENSE SERVICE PUBLIC FEDERAL ECONOMIE, P.M.E., CLASSES MOYENNES ET ÉNERGIE	FEDERALE OVERHEIDSDIENST JUSTITIE FEDERALE OVERHEIDSDIENST DEFENSIE FEDERALE OVERHEIDSDIENST ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE
_____	_____
Avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités	Voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten
PHILIPPE, Roi des belges,	FILIP, Koning der Belgen,
A tous, présents et à venir, SALUT.	<i>Aan allen die nu zijn en hierna wezen zullen,</i> ONZE GROET.
Vu l'analyse d'impact de la réglementation réalisée conformément aux articles 6 et 7 de la loi du 15 décembre 2013 portant des dispositions diverses en matière de simplification administrative;	Gelet op de impactanalyse van de regelgeving uitgevoerd overeenkomstig de artikelen 6 en 7 van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;
Vu la consultation publique, tenue du XX au XX ;	Gelet op de openbare raadpleging die werd gehouden van XX tot XX;
Vu l'avis de l'Autorité de protection des données du XXX ;	Gelet op het advies van de Gegevensbeschermingsautoriteit van XXX;

Vu l'avis de l'Organe de contrôle de l'information policière ;	Gelet op het advies van het Controleorgaan op de politionele informatie;
Vu l'avis du Comité Permanent R;	Gelet op het advies van het Vast Comité I;
Vu la consultation du X au X du Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision;	Gelet op de raadpleging vanaf X tot X van het Interministerieel Comité voor Telecommunicatie en Radio-omroep en Televisie;
Vu l'accord du Comité de concertation du XX;	Gelet op het akkoord van het Overlegcomité van XX;
Vu l'avis XXX du Conseil d'État, donné le XX/XX/XXXX, en application de l'article 84, § 1 ^{er} , alinéa 1 ^{er} , 2°, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973 ;	Gelet op het advies XXX van de Raad van State, gegeven op XX/XX/XXXX, met toepassing van het artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;
Sur la proposition de la Ministre des Télécommunications, du Ministre de la Justice, et de la Ministre de la Défense,	Op de voordracht van de Minister van Telecommunicatie, van de minister van Justitie, en van de minister van Defensie,
NOUS AVONS ARRETE ET ARRETONS :	HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:
CHAPITRE 1^{er} - Disposition générale	HOOFDSTUK 1 - Algemene bepaling
Article 1^{er}. La présente loi règle une matière visée à l'article 74 de la Constitution.	Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.
CHAPITRE 2 - Modifications à la loi du 13 juin 2005 relative aux communications électroniques	HOOFDSTUK 2 - Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2. A l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, au lieu du 74°, annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un 74° rédigé comme suit :	Art. 2. In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, in de plaats van de bepaling onder 74°, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende bepaling onder 74° ingevoegd:
"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."	"74° "Oproep poging zonder resultaat" : een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord."
Art. 3. Dans l'article 9 de la loi du 13 juin 2005 relative aux communications électroniques, le paragraphe 7 est abrogé.	Art. 3. In artikel 9 van de wet van 13 juni 2005 betreffende de elektronische communicatie wordt paragraaf 7 opgeheven.
Art. 4. Dans l'article 122 de la même loi, les modifications suivantes sont apportées :	Art. 4. In artikel 122 van dezelfde wet worden de volgende wijzigingen aangebracht:
1° Dans le paragraphe 1 ^{er} :	1° In paragraaf 1:
- Le mot "finals" est remplacé par le mot "finaux";	- Wordt in de Franstalige versie het woord "finals" vervangen door het woord "finaux";
- L'alinéa 2 est supprimé ;	- Wordt het tweede lid geschrapt;
2° Dans le paragraphe 2 :	2° In paragraaf 2:
- l'alinéa 1 ^{er} est remplacé par ce qui suit :	- wordt het eerste lid vervangen als volgt:";
"§2. Par dérogation au § 1 ^{er} , 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."	"§ 2. In afwijking van § 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".
- 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" ;	- worden in het tweede lid 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";

3° Dans le paragraphe 3:	3° In paragraaf 3:
- dans l'alinéa 1 ^{er} , 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 du RGPD" ;	- worden in het eerste lid, 2° 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 van de AVG";
- dans l'alinéa 1 ^{er} , 3°, les mots "utilisateurs finals la possibilité de retirer le consentement donné de manière simple" sont remplacés par les mots "utilisateurs finaux la possibilité de retirer le consentement donné facilement et à tout moment." ;	- worden in het eerste lid, 3° de woorden "op eenvoudige wijze" vervangen door de woorden "makkelijk en te allen tijde";
- 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" ;	- worden in het tweede lid 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° Le paragraphe 4 est remplacé comme suit:	4° Paragraaf 4 wordt vervangen als volgt:
"§ 4. Pour l'application du présent paragraphe, une fraude est 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, commis par le biais de l'utilisation d'un service de communications électroniques.	"§ 4. Voor de toepassing van deze paragraaf bestaat fraude in een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of het contract en om zichzelf of iemand anders een ongeoorloofd voordeel te doen, via het gebruik van een elektronische-communicatiedienst.
Pour l'application du présent paragraphe, une utilisation malveillante du réseau est une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages.	Voor de toepassing van deze paragraaf bestaat kwaadwillig gebruik van het netwerk in een gebruik van het netwerk teneinde zijn contactpersoon te ontrieven of schade te berokkenen.
Par dérogation au § 1 ^{er} , sans prendre connaissance du contenu des communications et dans le seul but de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications	In afwijking van § 1, zonder kennis te nemen van de inhoud van de communicatie en met als enig doel een vermoed geval van fraude of van kwaadwillig gebruik van een elektronische-communicatienetwerk op te

électroniques, en ce compris identifier son origine, les opérateurs :	sporen en te analyseren, inclusief de herkomst ervan:
1° conservent les données de localisation et les autres données de trafic nécessaires à cette fin, le temps nécessaire à cette fin et au minimum quatre mois ;	1° bewaren de operatoren de locatiegegevens en andere verkeersgegevens die daartoe nodig zijn, gedurende de tijd die ervoor nodig is en minstens vier maanden;
2° traitent les données de trafic nécessaires à cette fin, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.	2° verwerken de operatoren de noodzakelijke gegevens daartoe, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.
Lorsqu'un opérateur a détecté une fraude potentielle ou avérée ou une utilisation malveillante potentielle ou avérée du réseau, il prend les mesures appropriées, compte tenu des possibilités techniques les plus récentes, pour éviter que l'utilisateur final ne subisse un préjudice ou ne soit importuné.	Wanneer een operator een mogelijk of bewezen geval van fraude of een mogelijk of bewezen geval van kwaadwillig gebruik van het netwerk heeft opgespoord, neemt hij de gepaste maatregelen, rekening houdend met de meest recente technische mogelijkheden, om te vermijden dat de eindgebruiker schade ondervindt of wordt ontriefd.
Afin d'établir une utilisation malveillante d'un réseau de communications électroniques et de retrouver son auteur, les opérateurs conservent pendant 12 mois les données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles.	Om kwaadwillig gebruik van een elektronisch communicatienetwerk vast te stellen en de dader ervan te vinden, bewaren de operatoren gedurende 12 maanden de verkeersgegevens in verband met de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten.
Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et des Autorité de protection des données compétentes:	De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, bepalen:
1° les données de trafic visées aux alinéas 3 et 5 ;	1° de verkeersgegevens bedoeld in het derde en vijfde lid;
2° les actions que l'opérateur doit ou peut entreprendre lorsqu'il détecte une fraude présumée ou avérée ou une utilisation malveillante présumée ou avérée du réseau.	2° de acties die de operator moet of mag ondernemen wanneer hij een vermoed of bewezen geval van fraude of van kwaadwillig gebruik van het netwerk heeft opgespoord.
Les données visées aux alinéas 3 et 5 sont communiquées aux autorités compétentes en cas d'infraction présumée."	De gegevens bedoeld in het derde en vijfde lid worden meegedeeld aan de bevoegde autoriteiten in geval van vermoed misdrijf."
5° Un paragraphe 4/1 est inséré, rédigé comme suit :	5° Een paragraaf 4/1 wordt ingevoerd, luidend:

<p>“§ 4/1. Par dérogation au § 1er, les opérateurs conservent et traitent 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.</p>	<p>“§ 4/1. In afwijking van § 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om de veiligheid en correcte werking van hun netwerken en diensten voor elektronische communicatie 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.</p>
<p>Ils les conservent pour une durée de douze mois. Ils peuvent les conserver pour une durée plus longue, qui est limitée au strict nécessaire.”</p>	<p>Zij bewaren deze voor een duur van twaalf maanden. Zij kunnen ze voor een langere periode bewaren, die beperkt is tot het strikt noodzakelijke.”</p>
<p>6° Un paragraphe 4/2 est inséré, rédigé comme suit :</p>	<p>6° Een paragraaf 4/2 wordt ingevoerd, luidende:</p>
<p>“§ 4/2. Par dérogation au § 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation légale dans leur chef, pour la durée requise à cette fin.”</p>	<p>“§ 4/2. In afwijking van § 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een wettelijke verplichting die op hen rust, voor de daartoe benodigde duur.”</p>
<p>7° Le paragraphe 5 est remplacé comme suit :</p>	<p>7° Paragraaf 5 wordt vervangen als volgt:</p>
<p>“§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 à données de trafic ou de localisation et par les membres de sa Cellule de coordination. “</p>	<p>“§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 met verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel. “</p>
<p>8° Dans le paragraphe 6, les mots “L’Institut” sont remplacé par les mots “L’Institut, le Service de médiation pour les télécommunications,”.</p>	<p>8° In paragraaf 6 worden de woorden “het Instituut” vervangen door de woorden “het Instituut, de Ombudsdienst voor telecommunicatie,”.</p>
<p>9° Il est inséré un paragraphe 7, rédigé comme suit :</p>	<p>9° Er wordt een paragraaf 7 ingevoegd, luidende :</p>
<p>“§7. Cet article ne porte pas préjudice à l’article 127/1.”</p>	<p>“§ 7. Dit artikel doet geen afbreuk aan artikel 127/1.”</p>

Art. 5. À l'article 123 de la même loi, les modifications suivantes sont apportées	Art. 5. In artikel 123 van dezelfde wet worden de volgende wijzigingen aangebracht:
1° L'alinéa 1 ^{er} est remplacé comme suit:	1° de eerste paragraaf wordt vervangen als volgt:
“§ 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. 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° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées le temps nécessaire à cette fin ;	1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;
2° lorsque cela est nécessaire pour déceler des fraudes ou l'utilisation malveillante du réseau, les données étant conservées le temps nécessaire à cette fin ou ;	2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is; of;
3° lorsque les données ont été rendues anonymes, ou ;	3° wanneer de gegevens anoniem gemaakt zijn, of;
4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation, ou ;	4° wanneer de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens, of;
5° lorsque le traitement est nécessaire pour répondre à une obligation légale dans le chef de l'opérateur. ”	5° wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting in hoofde van de operator.”
2° Dans le paragraphe 2 :	2° In paragraaf 2:
- Dans le 1°, e), les mots “définitivement ou temporairement” sont abrogés ;	- Worden in het 1°, e), de woorden “definitief of tijdelijk” opgeheven;
- Dans le 2°, alinéa 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	- Worden in het 2°, tweede lid, 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

consentement au sens de l'article 4 du RGPD".	woorden "de toestemming in de zin van artikel 4 van de AVG".
3° Le paragraphe 4, alinéa 1 ^{er} est remplacé par ce qui suit :	3° Paragraaf 4, eerste lid, wordt vervangen als volgt:
"§4. 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 à données de trafic ou de localisation, ou par la Cellule de coordination de l'opérateur visée à l'article 127/3." ;	"§4. 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 met verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator waarvan sprake in artikel 127/3.";
4° Il est inséré un paragraphe 6, rédigé comme suit:	4° Er wordt een paragraaf 6 ingevoegd, luidende :
"§ 6. Cet article ne porte pas préjudice à l'article 127/1.".	"§ 6. Dit artikel doet geen afbreuk aan artikel 127/1.".
Art. 6. L'article 125, § 2, de la même loi est abrogé.	Art. 6. Artikel 125, § 2, van dezelfde wet wordt opgeheven.
Art. 7. Dans l'article 126 de la même loi, les modifications suivantes sont apportées :	Art. 7. In artikel 126 van dezelfde wet, worden de volgende wijzigingen aangebracht:
1° Le paragraphe 1er est remplacé comme suit:	1° Het paragraaf 1 wordt vervangen als volgt:
"§1. 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 de souscription de l'abonné ainsi que les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, pour autant qu'ils traitent ou génèrent ces données dans le cadre de la fourniture des réseaux ou services de communications concernés.	"§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 leveren, de abonnementsgegevens van de abonnee alsook de technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, op voorwaarde dat ze deze gegevens in het kader van de verstrekking van de communicatienetwerken of -diensten in kwestie verwerken of genereren.
Le présent article ne porte pas sur le contenu des communications.	Dit artikel heeft geen betrekking op de inhoud van de communicatie.

Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1.	Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.
Les données visées au présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.	De in dit artikel beoogde gegevens worden bewaard vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.
Par dérogation à l'alinéa 3, les adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service, sont conservées jusqu'à douze mois après la fin de la session."	In afwijking van het derde lid worden de andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst, tot twaalf maanden na het einde van de sessie bewaard."
2° Le paragraphe 2 est remplacé comme suit:	2° De tweede paragraaf wordt vervangen als volgt:
"§ 2. Le Roi fixe après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver ainsi que les exigences auxquelles ces données doivent répondre."	"§ 2. De Koning bepaalt, na advies van de bevoegde Gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens alsook de vereisten waaraan deze gegevens moeten beantwoorden."
Art. 8. Dans la même loi, un article 126/1 est inséré comme suit :	Art. 8. In dezelfde wet, wordt een artikel 126/1 ingevoegd, luidende :
"126/1. §1 ^{er} . Sans préjudice du RGDP 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 au paragraphe 2, pour les zones géographiques visées au paragraphe 3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans le présent article.	"126/1. §1. Onverminderd de AVG en de wet van 30 juli 2018, dienen de operatoren die aan de eindgebruikers elektronische communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische communicatienetwerken aanbieden, de in paragraaf 2 bedoelde gegevens voor de geografische zones bedoeld in paragraaf 3, te bewaren, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in huidig artikel.
Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communication concernés.	Elke operator bewaart de door hem gegenereerde of verwerkte gegevens in het kader van de verstrekking van de betrokken communicatiediensten en -netwerken.
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	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

sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.	openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.
§2. Les données visées au paragraphe 1 ^{er} sont les suivantes:	§ 2. De gegevens bedoeld in paragraaf 1 zijn:
1° les données 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 ;	1° de gegevens 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;
2° les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination ;	2° de communicatiegegevens, met uitzondering van de inhoud, en met inbegrip van hun herkomst en hun bestemming;
3° les données des appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés ;	3° de gegevens van oproep pogingen zonder resultaat, voor zover die gegevens in het kader van de aanbidding van de bedoelde communicatiediensten ;
i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs ; ou	i° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren; of
ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.	ii° wat de internetgegevens betreft, door deze operatoren worden gelogd.
Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre et 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 données à conserver et peut fixer les exigences auxquelles ces données doivent répondre.	De Koning bepaalt, 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 bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens en kan de vereisten waaraan deze gegevens moeten beantwoorden bepalen.
§ 3. Les zones géographiques dans lesquelles sont conservées les données visées au paragraphe 2 sont les suivantes :	§ 3. De geografische zones waarbinnen de gegevens bedoeld in paragraaf 2 bewaard worden, zijn de volgende:
1° la zone géographique composée des :	1° de geografische zones bestaande uit:
- arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées durant l'année sur une moyenne des trois années calendriers précédentes celle en cours ;	- de gerechtelijke arrondissementen waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drievoorbij kalenderjaren;

<ul style="list-style-type: none"> - zones de police, dans lesquelles, au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers précédentes celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédente celle en cours, moins de 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an sur une moyenne de trois années précédente celle en cours ont été constatées. 	<ul style="list-style-type: none"> - de politiezones waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren.
Dans l'hypothèse visée au 1 ^{er} tiret, le délai de conservation des données visées au paragraphe 2 est de :	In het geval bedoeld in het eerste streepje bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:
a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers précédentes celle en cours;	a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours;	b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
c) 12 mois, s'il y a 7 ou plus de 7 d'infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours.	c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de 3 voorbije kalenderjaren.
Dans l'hypothèse visée au deuxième tiret, le délai de conservation des données visées au paragraaf 2 est de :	In het geval bedoeld in het tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2 :
a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers précédentes celle en cours;	a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours;	b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.
c) 12 mois, s'il y a 7 ou plus de 7 infractions visées à l'article 90ter du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours.	c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.
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 5.	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 5 bereikt.
Les statistiques utilisées proviennent de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police.	De gebruikte statistieken zijn afkomstig van de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet op het politieambt.
La direction visée à l'article 44/11 de la loi sur la fonction de police transmet chaque année, à la date déterminée par le Roi, ces statistiques à l'Organe de contrôle de l'information policière qui, dans les [quinze] jours après leur réception, vérifie leur exactitude et en informe le service désigné par le Roi.	De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, zendt jaarlijks op de door de Koning vastgestelde datum deze statistieken toe aan het Controleorgaan op de politionele informatie dat, binnen de [vijftien] dagen na ontvangst, de juistheid ervan controleert en de door de Koning aangewezen dienst ervan in kennis stelt.
2° Toutes les zones 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 qu'un niveau d'au moins 3 perdure pour ces zones.	2° Alle zones waar het algemene dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2° van de wet van 10 juli 2006 betreffende de dreigingsanalyse, 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 dreigingsanalyse, en zolang niveau 3 blijft bestaan.
3° Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, à savoir:	3° De gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation ;	a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek;
b) les gares au sens de l'article 2, 5° de la loi du 27 avril 2018 sur la police des chemins de fer ;	b) de spoorwegstations in de zin van artikel 2, 5° van de Wet van 27 april 2018 houdende de spoorwegpolitie;
c) les stations de métro et de pré-métro ;	c) de metro- en de pre-metrostations ;
d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil, 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, et entités exploitant les installations annexes se trouvant dans les aéroports ;	d) de luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, 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, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden,
e) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution ;	e) de gebouwen bestemd voor de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;
f) les bâtiments affectés à la police locale et à la police fédérale ;	f) de gebouwen bestemd voor de lokale en de federale politie;
g) les bâtiments affectés à l'administration des douanes et accises ;	g) de gebouwen bestemd voor de administratie van douane en accijnzen;
h) les communes dans lesquelles se trouvent des domaines militaires ;	h) de gemeenten waar zich militaire domeinen bevinden;
i) 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 ;	i) de gevangenen in de zin van artikel 2, 15°, van de Basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gesteld, 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;
j) les maisons de transition visées dans la loi du 17 mai 2006 relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine ;	j) de transitiehuizen als bedoeld in de wet van 17 mei 2006 betreffende de externe rechtspositie van de veroordeelden tot een vrijheidsstraf en de aan het slachtoffer toegekende rechten in het raam van de strafuitvoeringsmodaliteiten;

k) les armuriers et les stands de tir au sens de l'article 2, points 1 et 19 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes ;	k) de wapenkamers en schietstanden zoals bedoeld in artikel 2, punten 1 en 19 van de Wet van 8 juni 2006 houdende de economische en individuele activiteiten met wapens;
l) 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 ;	l) de faciliteiten 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;
m) les établissements SEVESO visés dans l'accord de coopération du 16 février 2016 entre l'Etat 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 ;	m) de SEVESO-inrichtingen zoals bedoeld in 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;
n) les communes dans lesquelles il y a une ou plusieurs infrastructures critiques visées dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques;	n) de gemeenten waar zich kritieke infrastructuur bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur;
o) le réseau utilisé par la S.A. Astrid et ses infrastructures ainsi que le réseau et les infrastructures 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 ;	o) het door de N.V. Astrid gebruikte netwerk en haar infrastructuur, evenals het netwerk en het beveiligde en versleutelde communicatie- en informatiesysteem 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;
p) les réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de service essentiels désignés sur 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 ;	p) de informatienetwerken en –systemen die de verlening van essentiële diensten van operatoren van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid;
q) le cas échéant, les autres zones fixées par arrêté royal.	q) in voorkomend geval, de andere zones vastgesteld bij Koninklijk besluit.
4° Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays	4° De zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het

ou pour les besoins essentiels de la population, à savoir :	land of de essentiële behoeften van de bevolking, met name:
a) en matière d'ordre public, les zones neutres et les cabinets ministériels ;	a) voor de openbare orde, de neutrale zones en de ministeriële kabinetten;
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'Etat et le Service général du Renseignement et de la sécurité sur proposition du Ministre de la Justice et de la Défense et approuvée par le Conseil national de sécurité ;	b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden die zijn opgenomen in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;
c) pour le transport, les autoroutes et les parkings publics attenants ;	c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;
d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances :	d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnances:
i) les assemblées législatives au sens de l'article 1 ^{er} de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution ;	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) les maisons communales et les hôtels de ville ;	ii) de gemeentehuizen ;
iii) les sièges des conseils provinciaux ;	iii) de zetels van de provincieraden;
iv) le palais royal ;	iv) het koninklijk paleis;
v) les domaines royaux ;	v) de koninklijke domeinen;
vi) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution ;	vi) de gebouwen toegewezen aan de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;
vii) les communes dans lesquelles se trouvent des domaines militaires ;	vii) de gemeenten waar zich militaire domeinen bevinden;
viii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu' à la Sûreté de l'Etat ;	viii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
e) pour ce qui concerne l'intégrité du territoire national les communes frontalières;	e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

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 :	f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:
i) les hôpitaux au sens de l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soin ;	i) de ziekenhuizen zoals bedoeld in artikel 2 van de Gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;
ii) la Banque nationale de Belgique;	ii) de Nationale Bank van België;
g) le cas échéant, les autres zones fixées par arrêté royal.	g) in voorkomend geval, de andere zones vastgesteld bij koninklijk besluit.
5° Les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national, à savoir :	5° De zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, met name:
a) les ambassades et les représentations diplomatiques ;	a) de ambassades en diplomatieke vertegenwoordigingen;
b) les bâtiments affectés à l'Union Européenne ;	b) de gebouwen bestemd voor de Europese Unie;
c) les bâtiments et infrastructures affectés à l'OTAN ;	c) de gebouwen en de infrastructuur bestemd voor de NAVO;
d) les bureaux des institutions de l'Espace économique européen ;	d) de kantoren van de instellingen van de Europese Economische Ruimte;
e) les bureaux des Nations unies ;	e) de kantoren van de Verenigde Naties;
f) le cas échéant, les autres zones fixées par arrêté royal.	f) in voorkomend geval, de andere zones vastgesteld bij Koninklijk besluit.
Chaque autorité compétente dans l'une des matières visées aux points 1° à 5° transmet chaque année à la date déterminée par le Roi et au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.	Elke autoriteit die bevoegd is voor een van de in de punten 1 tot en met 5 bedoelde aangelegenheden deelt jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de operationele tenuitvoerlegging van dit lid.
Ces autorités informent sans délai 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 au paragraphe 1 ^{er} dans cette zone.	Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze

	zone zo spoedig mogelijk kan worden beëindigd.
Chaque année et chaque fois qu'il est informé d'une modification, le service désigné par le Roi met à jour la liste des zones géographiques soumises à l'obligation de conservation et transmet cette liste aux opérateurs.	Elk jaar en telkens wanneer hij van een wijziging in kennis wordt gesteld, werkt de door de Koning aangewezen dienst de lijst van de onder de geografische gebieden waar de gegevens moeten bewaard worden bij en zendt hij deze lijst door aan de operatoren.
A l'exception de la liste des lieux visés à l'alinéa 1 ^{er} , point 4°, b), mise 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 la liste actualisée des zones où une conservation de données est obligatoire.	Met uitzondering van de in het eerste lid, punt 4°, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten ter beschikking van het vast Comité I wordt gesteld, stelt de Koning aangewezen dienst de bijgewerkte lijst van zones waar de bewaring van gegevens verplicht is, ter beschikking van het Controleorgaan van de politionele informatie.
La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1 ^{er} , point 1°.	De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°.
§ 4. Les opérateurs conservent les données pour toutes les communications effectuées à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone.	§ 4. De operatoren bewaren de gegevens voor alle communicaties die vanuit of naar een geografisch gebied als bedoeld in paragraaf 3 worden gevoerd.
Lorsqu'un utilisateur final entre dans une zone visée au paragraphe 3 ou sort de cette zone, les seules données conservées sont celles traitées ou générées lorsqu'il se trouve dans cette zone.	Wanneer een eindgebruiker een in paragraaf 3 bedoelde zone binnengaat of deze zone verlaat, worden alleen de gegevens bewaard die zijn verwerkt of gegenereerd wanneer hij zich in deze zone bevond.
Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée au paragraphe 3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent à cet effet la localisation satellitaire d'un équipement terminal.	Om te bepalen of eindapparatuur zich in een geografisch gebied als bedoeld in paragraaf 3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens die beschikbaar zijn. Zij maken hiervoor gebruik van de satellietlocatie van eindapparatuur.
Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entière de la zone concernée tout en	Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de

limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.	bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.
§ 5. 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 :	§ 5. 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 bevoegde gegevensbeschermingsautoriteiten en van het Instituut, het volgende bepalen:
- les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées au paragraphe 3 ;	- de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones;
- la liste des différentes autorités compétentes dans les matières visées au paragraphe 3, alinéa 1 ^{er} , points 2° à 5° ;	- de lijst van de verschillende autoriteiten die bevoegd zijn voor de in paragraaf 3, eerste lid, punten 2° tot en met 5° bedoelde aangelegenheden ;
- les modalités de communication des informations par les autorités compétentes vers le 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 1 ^{er} ;	- de procedures voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de procedures 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;
- s'il y échet, les zones géographiques additionnelles visées au paragraphe 3, alinéa 1 ^{er} , points 3°, q), 4°, g) et 5° f).	- in voorkomend geval, de bijkomende geografische zones bedoeld in paragraaf 3, eerste lid, punten 3°, q), 4° g) en 5°, f).
L'arrêté royal visé à l'alinéa 1 ^{er} , 4 ^{ème} tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1 ^{er} 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.	Elke drie jaar dient het koninklijk besluit bedoeld in het eerste lid, 4e streepje te worden hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 voor wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt."
§ 6. 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	§ 6. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité voor Inlichtingen en Veiligheid, en van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, jaarlijks een evaluatieverslag uit aan de Kamer van

présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 5, afin de vérifier si des dispositions doivent être adaptées.	volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde Koninklijk Besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.
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 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1 ^{er} , points 3° à 5° et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.	In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5, bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.
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.	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
Ce rapport est envoyé à l'Organe de contrôle de l'information policière.	Dit evaluatierapport wordt gestuurd naar het controleorgaan op de politionele informatie.
Pour la première application du présent article :	Bij de eerste toepassing van huidig artikel:
- les opérateurs concernés le mettent en œuvre dans les trois mois après l'entrée en vigueur de l'arrêté royal visé au paragraphe 2, alinéa 2;	- leggen de betrokken operatoren dit artikel ten uitvoer binnen drie maanden na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 2, tweede lid;
- les autorités compétentes visées au paragraphe 3, alinéa 2 transmettent les informations nécessaires au service désigné par le Roi le mois qui suit l'entrée en vigueur de la loi.”.	- delen de paragraaf 3, tweede lid bedoelde bevoegde autoriteiten de nodige gegevens mee aan de door de Koning aangewezen dienst op de maand volgend op de inwerkingtreding van de wet.”.
Art. 9. Dans la même loi, l'article 127 est remplacé par ce qui suit :	Art. 9. In dezelfde wet, wordt het artikel 127 vervangen als volgt:
“Art. 127. § 1 ^{er} . Les opérateurs identifient leurs abonnés ou collectent et conservent les données nécessaires pour que les autorités qui sont habilitées à obtenir cette identité puissent les identifier.	“Art. 127. § 1. De operatoren identificeren hun abonnees of verzamelen en bewaren de nodige gegevens opdat de autoriteiten die gemachtigd zijn om deze identiteit te verkrijgen, hen kunnen identificeren.

Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1.	Deze gegevens en documenten worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.
Les données et documents collectés en vertu du présent article sont conservés à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.	De gegevens en documenten vergaard krachtens dit artikel, worden bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is aan de hand van de gebruikte dienst.
§2. Lorsque l'abonné présente un document d'identification comprenant le numéro de registre national, l'opérateur, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.	§ 2. Wanneer de abonnee een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.
Afin d'identifier l'abonné, l'opérateur ou le canal de vente de services de communications électroniques peut réaliser, de manière automatique, une comparaison entre les paramètres biométriques sur la photo de la pièce d'identité de l'abonné et ceux de son visage.	Teneinde de abonnee te identificeren, kan de operator of het verkoopkanaal van elektronische-communicatiediensten automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identiteitsstuk van de abonnee en deze van zijn gezicht.
Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur ou à l'entreprise fournissant un service d'identification.	Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator of naar de onderneming die een identificatiedienst verstrekt.
Si une introduction directe dans les systèmes informatiques de l'opérateur ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.	Indien een rechtstreekse invoer in de computersystemen van de operator of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.
L'opérateur conserve une copie des documents d'identification autres que la carte d'identité électronique belge.	De operator bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.
§3. Le Roi peut, après avis des Autorités de protection des données compétentes et de l'Institut, déterminer les modalités	§3. De Koning kan, na advies van de bevoegde gegevensbeschermingsautoriteiten en het

d'identification de l'utilisateur final, et entre autres :	Instituut, de nadere bepalingen voor identificatie van de eindgebruiker vastleggen, en onder andere:
1° déterminer si l'opérateur doit lui-même identifier ses abonnés ou s'il peut seulement rendre cette identification possible ;	1° bepalen of de operator zelf zijn abonnees moet identificeren of louter deze identificatie mogelijk moet kunnen maken;
2° déterminer les méthodes d'identification que les opérateurs peuvent utiliser, y compris soumettre une méthode d'identification proposée par un opérateur à une autorisation préalable du ministre et du ministre de la Justice ;	2° de methodes voor identificatie bepalen die de operatoren kunnen gebruiken, inclusief een door een operator voorgestelde identificatiemethode onderwerpen aan een voorafgaande machtiging van de minister en van de minister van Justitie;
3° déterminer les données et documents d'identification à collecter et à conserver par l'opérateur ;	3° de door de operator te verzamelen en bewaren identificatiegegevens en -documenten bepalen;
4° imposer des obligations aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification et aux utilisateurs finaux, en vue de l'identification de ces derniers.	4° verplichtingen opleggen aan de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken en de eindgebruikers, met het oog op de identificatie van deze laatsten.
Sauf preuve contraire, l'abonné est présumé utiliser lui-même le service de communications électroniques.	Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.
§4. 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.	§ 4. 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
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."	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."
Art. 10. Dans la même loi, un article 127/1 est inséré comme suit :	Art. 10. In dezelfde wet, wordt een artikel 127/1 ingevoegd, luidende:
"Art 127/1, § 1er. Seules les autorités suivantes peuvent obtenir, via la Cellule de coordination visée à l'article 127/3 des opérateurs des données conservées en	"Art. 127/1. §1. Enkel de volgende autoriteiten mogen, via de in artikel 127/3 bedoelde Coördinatiecel, van de operatoren gegevens ontvangen die worden bewaard

vertu des articles 122, 123, 126, 126/1, et 127 pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent :	krachtens de artikelen 122, 123, 126, 126/1 en 127 om de doeleinden hieronder en volgens de vastgelegde voorwaarden die hen daartoe machtigen:
1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne;	1° de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd;
2° 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° 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 veiligheidsdienst;
3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale;	3° de autoriteiten belast met het verlenen van hulp aan personen, inclusief de Ombudsdienst voor telecommunicatie wat betreft het kwaadwillig gebruik van het netwerk, de hulpdiensten en de Cel Vermiste Personen van de federale politie;
4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi;	4° het Instituut in het kader van de uitvoering en de controle van deze wet;
5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service;	5° de autoriteiten bevoegd voor het onderzoek van een veiligheidsprobleem op het netwerk of van de dienst;
§2. L'Institut publie sur son site Internet des informations générales concernant l'accès des autorités visées au paragraphe premier aux données conservées en vertu des articles 122, 123, 126, 126/1 et 127.	§ 2. Het Instituut publiceert op zijn website algemene informatie betreffende de toegang tot gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 voor de in de eerste paragraaf bedoelde autoriteiten.
Art. 11. Dans la même loi, un article 127/2 est inséré comme suit :	Art. 11. In dezelfde wet, wordt een artikel 127/2 ingevoegd, luidende:
“Art. 127/2, § 1er. Le ministre et le ministre de la Justice font en sorte que des statistiques sur l'accès des autorités aux données conservées en vertu des articles 122, 123, 126, 126/1 et 127 soient transmises annuellement à la Chambre des représentants.	“Art. 127/2 § 1. De minister en de minister van Justitie zorgen ervoor dat jaarlijks statistieken met betrekking tot de toegang van de autoriteiten tot de gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 worden bezorgd aan de Kamer van volksvertegenwoordigers.

Ces statistiques comprennent notamment :	Die statistieken omvatten met name:
1° les cas dans lesquels des données ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;	1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;
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 ;	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° les cas dans lesquels des demandes de données n'ont pu être satisfaites.	3° de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.
Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.	Die statistieken mogen geen persoonsgegevens of vertrouwelijke informatie omvatten.
Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90decies du Code d'instruction criminelle.	De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens gevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90decies van het Wetboek van strafvordering moet uitbrengen aan het Parlement.
Le Roi détermine sur avis de l'Institut, les statistiques que les opérateurs transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.	De Koning bepaalt op advies van het Instituut, de statistieken die de operatoren jaarlijks bezorgen aan het Instituut en deze die het Instituut bezorgt aan de minister en aan de minister van Justitie.
§2. Les opérateurs font en sorte que les données qu'ils conservent pour leurs propres besoins et celles qu'ils conservent pour les autorités soient accessibles de manière illimitée à partir de la Belgique.	§ 2. De operatoren zorgen ervoor dat de gegevens die ze bewaren voor hun eigen behoeften en deze die ze bewaren voor de autoriteiten onbeperkt toegankelijk zijn vanuit België.
Ils veillent également à garantir la qualité de ces données et, pour ce qui concerne les données conservées pour les autorités, à ce qu'elles soient de la même qualité que les données sur le réseau.	Ze garanderen eveneens de kwaliteit van deze gegevens en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ervoor dat ze dezelfde kwaliteit hebben als de gegevens in het netwerk.
Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités.	De operatoren zijn in staat verbanden te leggen tussen de gegevens bewaard voor de autoriteiten.
§ 3. Pour ce qui concerne les données conservées pour les autorités, les opérateurs:	§ 3. Wat betreft de gegevens bewaard voor de autoriteiten, dienen de operatoren:

1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;	1° te garanderen dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;
2° conservent les données sur le territoire de l'Union européenne ;	2° de gegevens op het grondgebied van de Europese Unie te bewaren;
3° 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° te zorgen voor 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;
4° 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 du RGDP et sans préjudice d'autres dispositions légales.	4° mogen 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 van de AVG en onverminderd andere wettelijke bepalingen.
Pour ce qui concerne les données conservées pour leurs propres besoins ou pour les autorités, les opérateurs:	Wat betreft de gegevens bewaard voor hun eigen behoeften of voor de autoriteiten, dienen de operatoren:
1° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou rendent ces données anonymes ;	1° 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;
2° 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 105/1 ;	2° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 105/1;
3° 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, § 1 ^{er} , de manière manuelle ou de manière automatisée;	3° 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 automatische wijze;
4° assurent une traçabilité de l'exploitation des données conservées pour chaque	4° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze

demande d'obtention de ces données d'une autorité.	gegevens te verkrijgen vanwege een autoriteit.
La traçabilité visée à l'alinéa 1 ^{er} , 4 ^o , s'effectue à l'aide d'un journal.	De in het eerste lid, 4 ^o , bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.
L'opérateur prend les mesures nécessaires pour que chaque accès aux données qu'il conserve pour les autorités et chaque accès d'un membre de la Cellule de coordination visée à l'article 127/3 à d'autres données génère de manière automatisée un enregistrement dans le journal.	De operator neemt de nodige maatregelen opdat elke toegang tot de gegevens die hij bewaart voor de autoriteiten en elke toegang van een lid van de Coördinatiecel bedoeld in artikel 127/3 tot andere gegevens, automatisch wordt geregistreerd in het logboek.
Ce journal comprend également les informations et documents suivants :	Dit logboek bevat eveneens de volgende informatie en documenten:
1° l'identité de la personne ayant accédé aux données ;	1° de identiteit van de persoon die toegang heeft gehad tot de gegevens;
2° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande et la demande ;	2° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek en het verzoek;
3° 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.	3° 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.
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.	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.
Les données de ce journal sont conservées pendant une période de dix ans. A l'échéance de la période de conservation, les données du journal sont détruites.	De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.
L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal et, en particulier, pour empêcher toute manipulation non autorisée de ce dernier.	De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen en, in het bijzonder, om elke niet-toegestane handeling in verband met dat logboek te voorkomen.
Le Roi peut préciser, après avis des Autorités de protection des données compétentes et de l'Institut, les exigences à	De Koning kan, na advies van de Gegevensbeschermingsautoriteiten en van het Instituut, de eisen bepalen die de

respecter par les opérateurs concernant le journal.	operatoren in acht moeten nemen wat betreft het logboek.
Dans le cadre du contrôle de l'opérateur, l'Institut et les autorités de protection des données compétentes peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.	In het kader van de controle van de operator mogen het Instituut en de bevoegde gegevensbeschermingsautoriteiten mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.
§ 4. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2 ou 3, 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.	§ 4. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2 of 3, 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.
Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en compris le journal visé au paragraphe 3, alinéa 3.	Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 3, derde lid.
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.”.	Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.”.
Art. 12. Dans la même loi, un article 127/3 est inséré comme suit :	Art. 12. In dezelfde wet, wordt een artikel 127/3 ingevoegd, luidende:
“Art. 127/3. § 1 ^{er} . 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.	“Art. 127/3. § 1. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.
Ces autorités adressent leurs demandes à cette cellule.	Deze autoriteiten richten hun verzoeken tot deze cel.
Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, cette Cellule de coordination doit prévoir le même service pour chaque opérateur.	In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval moet deze Coördinatiecel voorzien in dezelfde dienst voor elke operator.
Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1 ^{er} . Ils peuvent cependant, sous leur surveillance et dans la	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

limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur.	het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.
Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.	De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.
Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.	Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.
§ 2. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met à la disposition de l'Institut, sur demande, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.	§ 2. Elke operator stelt een interne procedure op om te antwoorden op de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens betreffende de eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.
Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127.	Elke operator wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de AVG, voor de gegevens behandeld op basis van de artikelen 122, 123, 126, 126/1 en 127.
§3. Le Roi peut déterminer, après avis des autorités de protection des données compétentes et de l'Institut :	§3. De Koning kan na advies van de bevoegde gegevensbeschermingsautoriteiten, en van het Instituut het volgende bepalen:
1° les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité;	1° de vereisten waaraan de Coördinatiecel moeten beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid;
2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en ce compris lui imposer, le cas échéant, de faire l'objet d'un avis de sécurité positif ;	2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inclusief hem in voorkomend geval verplichten om het voorwerp uit te maken van een positief veiligheidsadvies;
3° si un avis de sécurité positif est imposé, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un officier de sécurité comme prévu à l'article 22quinquies, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ainsi que les règles qui s'appliquent en l'absence d'un tel officier ;	3° indien een positief veiligheidsadvies wordt opgelegd, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een veiligheidsofficier aan te stellen zoals bepaald in artikel 22quinquies, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

4° les règles permettant que les autorités belges qui ont besoin de connaître les coordonnées de la Cellule de coordination et de ses membres en soient informés ;	4° de regels die het mogelijk maken dat de Belgische autoriteiten die de contactgegevens van de Coördinatiecel en van de leden ervan moeten kennen, daarvan op de hoogte worden gebracht;
5° les autres règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles, y compris, le cas échéant et par autorité concernée :	5° de overige regels die de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen regelen, met inbegrip van, in voorkomend geval en per betrokken overheid:
a) le mode de transfert, la forme et le contenu des demandes et des réponses ;	a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;
b) le degré d'urgence de traitement des demandes ;	b) het dringendheidsniveau voor de behandeling van de verzoeken;
c) le délai de réponse;	c) de reactietermijn voor de antwoorden;
d) la disponibilité requise du service;	d) de vereiste beschikbaarheid van de dienst;
e) les modalités de test de la collaboration;	e) de modaliteiten voor het testen van de samenwerking;
f) les tarifs de rétribution de cette collaboration.	f) de tarieven van de vergoeding van die samenwerking.
Si nécessaire, le Roi peut prévoir des règles différentes selon 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 le lieu où ils opèrent leurs activités.”.	Indien nodig kan de Koning verschillende regels bepalen volgens verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en de plaats waar zij hun activiteiten uitvoeren.”.
Art. 13. Dans la même loi, l'article 127/4 est inséré comme suit :	Art. 13. In dezelfde wet, wordt het artikel 127/4 ingevoegd, luidende:
“Art. 127/4 Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les conditions dans lesquelles les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public enregistrent et conservent les données permettant l'identification des personnes concernées	“Art. 127/4. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de voorwaarden vast waaronder de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet openbaar beschikbaar zijn de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur

de l'équipement terminal ou du service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, en vue de la poursuite et la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence, en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	of van de gebruikte elektronische-communicatiedienst, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten en met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les mesures techniques et administratives imposées aux fournisseurs visées à l'alinéa 1 ^{er} , en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par les articles 46bis, 88bis, 90ter à 90decies, 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de technische en administratieve maatregelen vast die aan de aanbieders beoogd in het eerste lid worden opgelegd om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennismaken en opnemen van niet voor het publiek toegankelijke mogelijk te maken onder de voorwaarden bepaald door de artikelen 46bis, 88bis, 90ter tot 90decies, 464/13, 464/25 en 464/26 van het Wetboek van strafvordering, evenals de voorwaarden bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
Les fournisseurs visés à l'alinéa 1 ^{er} font en sorte que les données mentionnées à l'alinéa 1 ^{er} soient accessibles de manière illimitée depuis la Belgique.”	De aanbieders beoogd in het eerste lid zorgen ervoor dat de in het eerste lid van deze paragraaf vermelde gegevens onbeperkt toegankelijk zijn vanuit België.”
Art. 14. Dans la même loi, un article 127/5 est inséré comme suit :	Art. 14. In dezelfde wet, wordt een artikel 127/5 ingevoegd, luidende:
“Art. 127/5. §1 ^{er} . Sauf pour les systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, qui font l'objet de règles	“Art. 127/5. §1. Behalve voor de versleutelingssystemen die gebruikt kunnen worden om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen, welke onder

particulières au paragraphe 2, il est interdit de fournir ou d'utiliser un service ou un équipement qui empêche la réalisation des opérations suivantes:	specifieke regels vallen in paragraaf 2, is het verboden om een dienst of een toestel aan te bieden of te gebruiken waardoor de uitvoering van de volgende handelingen wordt verhinderd:
1° les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant ;	1° noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of de verstrekking van de identificatiegegevens van de oproeper;
2° l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;	2° de identificatie van de eindgebruiker, het opsporen en lokaliseren van niet voor het publiek toegankelijke communicatie onder de voorwaarden bepaald door het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;
3° les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	3° het afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie onder de voorwaarden bepaald door het Wetboek van strafvordering en door de wet van 30 november 1998. houdende regeling van de inlichtingen- en veiligheidsdiensten.
§ 2. Les dispositions du présent paragraphe dérogent à l'article 105/4.	§ 2. De bepalingen van deze paragraaf wijken af van artikel 105/4.
Le paragraphe 1er, alinéa 1er, 1°, est applicable aux systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	Paragraaf 1, eerste lid, 1°, is van toepassing op de versleutelingssystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen.
Les systèmes d'encryptage visés à l'alinéa 1er, ne peuvent pas empêcher la conservation par l'opérateur des données d'identification, de trafic ou de localisation pour les autorités, comme prévu dans la présente loi, le Code d'instruction criminelle ou la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	De in het eerste lid bedoelde versleutelingssystemen mogen niet verhinderen dat de operator voor de autoriteiten identificatie-, verkeers- of locatiegegevens bewaart, zoals bepaald in deze wet, het Wetboek van strafvordering of de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
Lorsqu'un opérateur a mis en place un système d'encryptage visé à l'alinéa 1er, il rend possible les opérations visées au paragraphe 1er, alinéa 1er, 2° et 3°, dans les [24 heures] à partir de la transmission d'une requête.	Wanneer een operator een versleutelingssysteem als bedoeld in het eerste lid heeft ingesteld, maakt hij de in paragraaf 1, eerste lid, 2° en 3° bedoelde handelingen mogelijk binnen [24 uur] na de verzending van het verzoekschrift.
Il rend possible la réalisation de ces opérations uniquement pour les	Hij maakt de uitvoering van deze handelingen enkel mogelijk voor de

communications visées dans la requête et qui sont postérieures à celle-ci.	communicatie waarop het verzoekschrift slaat alsook voor de communicatie die daarna volgt.
Toute clause contractuelle faisant obstacle au respect des obligations visées dans le présent paragraphe est interdite et nulle.	Elke contractuele clausule die de inachtneming van de in deze paragraaf beoogde verplichtingen belemmert, is verboden en nietig.
Art. 15. À l'article 145 de la même loi, les modifications suivantes sont apportées :	Art. 15. In artikel 145 van dezelfde wet worden de volgende wijzigingen aangebracht:
1° dans le paragraphe 1 ^{er} , les mots "127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, et 127" sont remplacés par les mots "126 à 127/5 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, 126, 126/1, 127 et 127/2 à 127/4."	1° in paragraaf 1, worden de woorden "127 en de ter uitvoering van de artikelen 32, 39, § 3, 47, en 127 genomen besluiten overtreedt." vervangen door de woorden "126 tot en met 127/5 en de ter uitvoering van de artikelen 32, 39, § 3, 47, 126, 126/1, 127 en 127/2 tot en met 127/4 genomen besluiten overtreedt."
2° au lieu du paragraphe 3 ^{ter} , annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un paragraphe 3 ^{ter} rédigé comme suit :	2° in de plaats van paragraaf 3 ^{ter} , vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3 ^{ter} ingevoegd :
« § 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 :	"§ 3 ^{ter} . Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft :
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;	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° 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. ».	2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt."
CHAPITRE 3 - Modifications à la loi du 17 janvier 2003 relative au statut du	HOOFDSTUK 3 – Wijzigingen van de wet van 17 januari 2003 met betrekking tot het

régulateur des secteurs des postes et des télécommunications belges.	statuut van de regulator van de Belgische post- en telecomunicatiesector
Art. 16. A l'article 14, § 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, un 2°/1 est introduit entre le 2° et le 3°, rédigé comme suit :	Art. 16. In artikel 14, § 2, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecomunicatiesector wordt een 2°/1 ingevoegd tussen de 2° en de 3°, luidend als volgt:
« 2°/1 peut demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions ; » .	“2°/1 kan het Instituut van de operatoren de identificatie-, verkeers- of locatiegegevens vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten;”
CHAPITRE 4 - Modifications du Code d'instruction criminelle	HOOFDSTUK 4 - Wijzigingen aan het Wetboek van strafvordering
Art. 17. Dans le Code d'instruction criminelle, un article 39quinquies est inséré comme suit:	Art. 17. In het Wetboek van strafvordering wordt een artikel 39quinquies ingevoerd, luidende:
“Art. 39quinquies. § 1. 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 88bis, §1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.	“Art. 39quinquies. § 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 noodzakelijke gegevens bedoeld in artikel 88bis, §1, eerste lid, die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.
L'ordre visé à l'alinéa 1er peut être donné, directement ou par l'intermédiaire du service de police désigné par le Roi, à :	Het bevel bedoeld in het eerste lid kan, rechtstreeks of via de door de Koning aangewezen politiedienst, gegeven worden aan:
- l'opérateur d'un réseau de communications électroniques ; et	- de operator van een elektronisch communicatienetwerk; en

<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - 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 elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.
La décision écrite et motivée mentionne:	De met redenen omklede en schriftelijke beslissing vermeldt:
<ul style="list-style-type: none"> - le nom du procureur du Roi qui ordonne la conservation ; 	<ul style="list-style-type: none"> - de naam van de procureur des Konings die de bewaring beveelt;
<ul style="list-style-type: none"> - l'infraction qui fait l'objet de l'ordre ; 	<ul style="list-style-type: none"> - het strafbare feit waarop het bevel betrekking heeft;
<ul style="list-style-type: none"> - les circonstances de fait de la cause qui justifient la conservation ; 	<ul style="list-style-type: none"> - de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen;
<ul style="list-style-type: none"> - 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 ; 	<ul style="list-style-type: none"> - 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;
<ul style="list-style-type: none"> - le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées ; 	<ul style="list-style-type: none"> - in voorkomend geval, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden;
<ul style="list-style-type: none"> - la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement ; 	<ul style="list-style-type: none"> - de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevel, onverminderd een hernieuwing;
<ul style="list-style-type: none"> - la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit. 	<ul style="list-style-type: none"> - de duur van bewaring van deze gegevens, die niet langer mag zijn dan zes maanden. Deze termijn kan schriftelijk worden verlengd.
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.	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. Les acteurs visés au § 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.	§ 2. De actoren bedoeld in § 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. 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.	§ 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.
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.	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 tot twintigduizend euro of met één van die straffen alleen.
§4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88bis.	§ 4. De toegang tot de overeenkomstig dit artikel bewaarde gegevens kan slechts met toepassing van artikel 88bis.
Art. 18. Dans l'article 88bis du même Code, inséré par la loi du 11 février 1991 et modifié en dernier lieu par la loi du 5 mai 2019, les modifications suivantes sont apportées :	Art. 18. In artikel 88bis, ingevoegd bij de wet van 11 februari 1991 en laatstelijk gewijzigd bij de wet van 5 mei 2019, worden de volgende wijzigingen aangebracht:
1° dans le paragraphe 1 ^{er} , alinéa 5, les mots "conformément au paragraphe 2" sont supprimés ;	1° In paragraaf 1, vijfde lid, worden de woorden "overeenkomstig paragraaf 2" geschrapt;
2° Paragraphe 3, inséré par la loi du 29 mai 2016, modifié par la loi du 5 mai 2019 et annulé par l'arrêt n° 57/2021 du 22 avril 2021 de la Cour Constitutionnelle, est rétabli dans la rédaction suivante :	2° Paragraaf 3, ingevoegd bij de wet van 29 mei 2016, gewijzigd bij de wet van 5 mei 2019 en vernietigd door arrest nr. 57/2021 van 22 april 2021 van het Grondwettelijk Hof, wordt hersteld als volgt:
"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.	"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.

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."	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."
CHAPITRE 5 - Modifications de la loi du 5 août 1992 sur la fonction de police	HOOFDSTUK 5 - Wijzigingen van de wet van 5 augustus 1992 op het politieambt
Art. 19. A l'article 42 de la loi du 5 août 1992 sur la fonction de police, modifié par la loi du 12 novembre 2017, les modifications suivantes sont apportées :	Art. 19. In artikel 42 van wet van 5 augustus 1992 op het politieambt, gewijzigd bij de wet van 12 november 2017, worden de volgende wijzigingen aangebracht:
1° Le mot "§1 ^{er} " est inséré au début de l'article ;	1° Het woord "§1" wordt ingevoegd aan het begin van het artikel;
2° L'article est complété par un paragraphe 2 rédigé comme suit:	2° Het artikel wordt aangevuld met een paragraaf 2 ingevoegd, luidende:
" § 2. Un officier de police judiciaire de la Cellule des 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.	"§ 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.
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	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

terminaison du réseau, concernant la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données, sont communiquées.	apparatuur, inclusief het netwerkaansluitpunt, betreffende de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan de opvordering, worden meegedeeld.
La réquisition est adressée par l'officier de police judiciaire visé à paragraphe 2, alinéa 1, à :	De vordering wordt via de officier van gerechtelijke politie bedoeld in paragraaf 2, eerste lid 1, gericht aan:
- l'opérateur d'un réseau de communications électroniques ; ou	- de operator van een elektronisch communicatienetwerk; of
- 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. “	- 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 elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.”
CHAPITRE 6 - Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité	HOOFDSTUK 6 - Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten
Art. 20. À l'article 3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les modifications suivantes sont apportées:	Art. 20. In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, worden de volgende wijzigingen aangebracht:
1° le 10° est complété par les mots “, quelle que soit la nature du destinataire ou du récepteur; ” ;	1° de bepaling onder 10° wordt aangevuld met de woorden “, ongeacht de aard van de bestemming of de ontvanger;”;
2° il est inséré un 10/1 , rédigé comme suit :	2° onder 10°/1° wordt een bepaling ingevoegd, luidende :
“10/1° "opérateur" : personne ou entreprise qui, sur le territoire belge, fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public”.	“10/1° “operator”: persoon of onderneming die op het Belgische grondgebied een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische communicatiedienst aanbiedt”.

Art. 21. A l'article 7 de la même loi, les mots ", chargée de la sécurité nationale," sont insérés entre les mots "La Sûreté de l'État" et "a pour mission".	Art. 21. In artikel 7 van dezelfde wet, worden de woorden “, belast met de nationale veiligheid,” ingevoegd tussen de woorden “Veiligheid van de Staat” en “heeft als opdracht”.
Art. 22. Dans l'article 11 de la même loi, les mots ", chargé de la sécurité nationale," sont insérés entre les mots "Renseignement et de la Sécurité" et "a pour mission".	Art. 22. In artikel 11 van dezelfde wet, worden de woorden “, belast met de nationale veiligheid,” ingevoegd tussen de woorden “Inlichting en Veiligheid” en “heeft als opdracht”.
Art. 23. A l'article 16/2, §1, les modifications suivantes sont apportées :	Art. 23. In artikel 16/2, §1, worden de volgende wijzigingen aangebracht :
1° A l'alinéa 1 ^{er} , les mots “de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques” sont abrogés;	1° In het eerste lid worden de woorden “van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst” opgeheven;
2° A l'alinéa 3, les mots “de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques” sont abrogés;	2° In het derde lid worden de woorden “van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst” opgeheven;
3° A l'alinéa 4, les mots “ou du fournisseur du service” sont abrogés.	3° In het vierde lid worden de woorden “of van de dienstenverstrekker” opgeheven.
Art. 24. Dans la même loi, un article 16/2/1 est inséré, rédigé comme suit :	Art. 24. In dezelfde wet wordt een artikel 16/2/1 ingevoerd, luidende:
“Art. 16/2/1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur pour procéder à la conservation des :	“Art. 16/2/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator voor het bewaren van :
1° données de trafic et de localisation de moyens de communications électroniques conservées au moment de la réquisition et qui font l'objet de celle-ci;	1° de verkeers- en lokalisatiegegevens van de elektronische communicatiemiddelen die op het ogenblik van de vordering worden bewaard en die het voorwerp uitmaken van de vordering;
2° données de trafic et de localisation qu'il génère et traite et qui font l'objet de la réquisition.	2° de verkeers- en lokalisatiegegevens die hij genereert en verwerkt en die het voorwerp uitmaken van de vordering.

La décision est effectuée par écrit par le dirigeant de service ou son délégué et est motivée.	De beslissing gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde en wordt met redenen omkleed.
En cas d'urgence, le dirigeant du service ou son délégué peut requérir cette conservation verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.	In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze bewaring mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.
La réquisition écrite mentionne :	De schriftelijke vordering vermeldt:
1° les personnes, les groupes de personnes, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation font l'objet de la conservation ;	1° de personen, groepen personen, geografische gebieden, communicatiemiddelen en/of gebruikswijzen waarvoor de verkeers- en lokalisatiegegevens moeten worden bewaard;
2° la durée de conservation des données qui ne peut excéder six mois sans préjudice de la possibilité de prolongation en suivant la même procédure.	2° de periode gedurende welke de gegevens worden bewaard, die niet langer mag zijn dan zes maanden, onverminderd de mogelijkheid van verlenging volgens dezelfde procedure.
Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.	De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.
Le Comité permanent R reçoit chaque mois du service de renseignement et de sécurité concerné une liste des réquisitions de conservation. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la méthode.	Het Vast Comité I ontvangt elke maand van de betrokken inlichtingen- en veiligheidsdienst een lijst van vorderingen tot bewaring. Indien er een onwettigheid vastgesteld wordt, beëindigt het Vast Comité I de methode.
Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.	Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.
Les données conservées par les opérateurs sur base du présent article sont détruites 12 mois après le début de leur conservation.	Gegevens die door operatoren op grond van dit artikel worden bewaard, worden 12 maanden na het begin van hun bewaring vernietigd.
Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs."	De Koning kan, op voorstel van de Minister van Justitie, de Minister van Defensie en de Minister bevoegd voor de elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen."

Art. 25. A l'article 18/2, §2, de la même loi, les mots "à 18/17" sont remplacés par les mots "à 18/17/1".	Art. 25. In artikel 18/2, §2, van dezelfde wet worden de woorden "tot 18/17" vervangen door de woorden "tot 18/17/1".
Art. 26. A l'article 18/3, §2, de la même loi, le 12° est abrogé.	Art. 26. In artikel 18/3, §2, van dezelfde wet wordt de bepaling onder 12° opgeheven.
Art. 27. À l'article 18/7 de la même loi, les modifications suivantes sont apportées :	Art. 27. In artikel 18/7 van dezelfde wet worden de volgende wijzigingen aangebracht:
1° Au paragraphe 1, 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";	1° In 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° Au paragraphe 1, 2°, les mots "d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques" sont abrogés;	2° In paragraaf 1 worden in de bepaling onder 2° de woorden "van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst" opgeheven;
3° Au paragraphe 1, 2°, les mots "la communication des factures afférentes aux abonnements identifiés," sont insérés entre les mots "afin de l'obtenir" et les mots "les données relatives à la méthode de paiement";	3° In paragraaf 1 worden in de bepaling onder 2° de woorden "de mededeling van de facturen met betrekking tot de geïdentificeerde abonnements," ingevoegd tussen de woorden "tot het bekomen van" en de woorden "de gegevens betreffende de betalingswijze";
4° Au paragraphe 3, alinéa 1, les mots "d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques" sont abrogés;	4° In paragraaf 3, eerste lid worden de woorden "van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst" opgeheven;
5° Au paragraphe 3, alinéa 2, les mots "le dirigeant du service" sont remplacés par les mots "le service concerné".	5° In paragraaf 3, tweede lid, worden de woorden "het diensthoofd" vervangen door de woorden "de betrokken dienst".

Art. 28. L'article 18/8 de la même loi est remplacé comme suit :	Art. 28. Het artikel 18/8 van dezelfde wet wordt vervangen als volgt:
“ Art. 18/8. § 1 ^{er} . 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, procéder ou faire procéder :	“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 te vorderen, overgaan of doen overgaan tot :
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;	1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;
2° à la localisation de l'origine ou de la destination de communications électroniques.	2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.
Dans les cas visés à l'alinéa 1 ^{er} 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.	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.
La nature de la décision est communiquée à l'opérateur.	De aard van de beslissing wordt meegedeeld aan de operator.
§ 2. Tout opérateur qui est requis de communiquer les données visées au § 1 ^{er} 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 proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les Communications électroniques dans ses attributions.	§ 2. Iedere operator die verzocht wordt de in § 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.
Toute personne visée à l'alinéa 1 ^{er} 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. “	Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro. “

Art. 29. A l'article 18/10, §4, alinéa 4, de la même loi, les mots "et 18/17" sont remplacés par les mots " , 18/17 et 18/17/1 " .	Art. 29. In artikel 18/10, §4, vierde lid, van dezelfde wet worden de woorden "en 18/17" vervangen door de woorden " , 18/17 en 18/17/1".
Art. 30. A l'article 18/17, §3, alinéa 1 ^{er} de la même loi, les mots "du réseau ou le fournisseur d'un service de communications électroniques" sont abrogés.	Art. 30. In artikel 18/17, § 3, eerste lid, van dezelfde wet, worden de woorden "van het netwerk of de verstrekker van een elektronische communicatiedienst" opgeheven.
Art. 31. Dans la même loi, il est inséré un article 18/17/1, rédigé comme suit :	Art. 31. In dezelfde wet wordt een artikel 18/17/1 ingevoerd, luidende:
"Art. 18/17/1. 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 pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.	"Art. 18/17/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid, de medewerking vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.
La réquisition est effectuée par écrit par le dirigeant du service et mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné visée à l'article 18/10 § 3, alinéa 3, selon le cas.	De vordering wordt schriftelijk gedaan door het diensthoofd en vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister bedoeld in artikel 18/10, §3, derde lid.
L'autorisation du dirigeant du service est transmise au ministre compétent.	De machtiging van het diensthoofd wordt overgemaakt aan de bevoegde minister.
Le service de renseignement et de sécurité concerné peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques pour transmettre la réquisition à tous les opérateurs concernés.	De betrokken inlichtingen- en veiligheidsdienst kan de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, om de vordering aan alle betrokken operatoren over te maken.
Le dirigeant du service peut requérir, par une décision écrite, des personnes dont il présume qu'elles ont une expertise	Het diensthoofd kan bij schriftelijke beslissing vorderen dat personen van wie hij veronderstelt dat zij over de nodige

technique utile de prêter leur concours à la mise en œuvre de cette méthode. Cette réquisition mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.	technische deskundigheid beschikken, medewerking verlenen bij de tenuitvoerlegging van deze methode. De vordering vermeldt, naargelang het geval, de aard van de instemming van de commissie, de aard van de instemming van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.
Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.	Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.
La méthode est autorisée pour une durée ne pouvant excéder 6 mois sans préjudice de la procédure visée à l'article 18/10, §5.	De methode wordt toegestaan voor een periode die niet langer mag zijn dan 6 maanden onverminderd de procedure bedoeld in artikel 18/10, §5.
Le service de renseignement et de sécurité concerné fait rapport à la commission tous les deux mois 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.	De betrokken inlichtingen- en veiligheidsdienst brengt om de twee maanden bij de Commissie verslag uit over de evolutie van de dreiging. In dit verslag worden de elementen belicht die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.
Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs.”.	De Koning kan, op voorstel van de Minister van Justitie, de Minister van Defensie en de Minister bevoegd voor de elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen.”.
CHAPITRE 7 - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	HOOFDSTUK 7 - Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
Art. 32. A l'article 84 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, il est inséré un paragraphe 1 ^{er} bis/1 rédigé comme suit :	Art. 32. In artikel 84 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, wordt een paragraaf 1bis/1 ingevoegd, luidende:
“§ 1 ^{er} bis/1. Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou	“§ 1bis/1. Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de

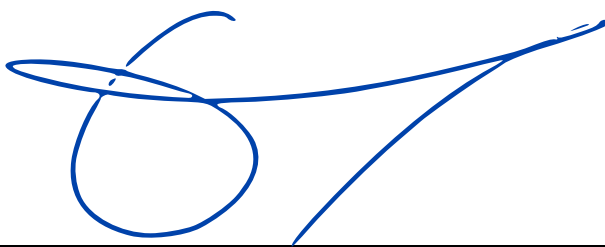
aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1 ^{er} , alinéa 2, de conserver les données visées au paragraphe 1 ^{er} , alinéa 1 ^{er} , qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.	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.
Les paragraphes 1 ^{er} , alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1 ^{er} .	Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.
Les acteurs visés au paragraphe 1 ^{er} , 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.	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.
L'auditeur ou, en son absence, l'auditeur adjoint fait part au juge d'instruction de l'ordre visé à l'alinéa 1 ^{er} au moment où il lui adresse sa demande d'autorisation préalable pour requérir la communication des données visées au paragraphe 1 ^{er} , alinéa 1 ^{er} . Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre ou s'il estime que l'ordre n'était pas légitime ou pas justifié, cet ordre s'éteint.”.	De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, bezorgt het in het eerste lid bedoelde bevel aan de onderzoeksrechter gelijktijdig met zijn verzoek tot voorafgaande toestemming om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel betrekking heeft of oordeelt dat het bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel.”.
CHAPITRE 8 - 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	HOOFDSTUK 8 - Wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten
Art. 33. 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	Art. 33. Artikel 11, § 1, van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere

avril 2014, est complété par un alinéa rédigé comme suit :	producten, vervangen bij de wet van 10 april 2014, wordt aangevuld met een lid, luidende:
<p>“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.</p> <p>À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d’identification à :</p> <p>1° l’opérateur d’un réseau de communications électroniques ; et</p> <p>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.</p>	<p>“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. Hiertoe mogen zij met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen van :</p> <p>1° de operator van een elektronisch communicatienetwerk; en</p> <p>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 elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.</p>
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. »	Onverminderd een eventuele delegatie, dient elk identificatieverzoek voorafgaand, door het diensthoofd van de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.”
CHAPITRE 9 - Modification 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 (« loi NIS »)	HOOFDSTUK 9 - Wijziging 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 (“NIS-wet”)
Art. 34. 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 comme suit :	Art. 34. 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. Dans le cadre de l’exercice de ses compétences, le CSIRT national prend	“Art. 62. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale

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.	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. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, le CSIRT national peut obtenir des opérateurs, au sens de l'article 2, 11° de la loi du 13 juin 2005 relative aux communications électroniques, des données d'identification, de trafic et de localisation conservées par ceux-ci.	§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e) van deze wet, kan het nationale CSIRT van de operatoren, als bedoeld in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, identificatie- en verkeers- en locatiegegevens die door hen worden bewaard, verkrijgen.
Pour ce faire, le CSIRT national respecte les règles et les procédures prévues par la loi du 13 juin 2005 relative aux communications électroniques.	Daartoe houdt het nationale CSIRT zich aan de regels en procedures bedoeld in de wet van 13 juni 2005 betreffende de elektronische communicatie.
Les fonctionnaires dirigeants du CSIRT national désignent expressément les personnes habilitées à solliciter ces informations auprès des opérateurs visés à l'alinéa 1 ^{er} et à les traiter.	De leidende ambtenaren van het nationale CSIRT wijzen uitdrukkelijk de personen aan die gemachtigd zijn om deze informatie op te vragen bij de operatoren bedoeld in het eerste lid en om ze te verwerken.
§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.	§ 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. 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.	§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.
Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de	De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit

procédures internes, au respect des conditions visées au présent article.”.	artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.”
Art. 35. 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 “des données de géolocalisation”.	Art. 35. In artikel 65, §2, van dezelfde wet worden de woorden “elektronische communicatiegegevens,” ingevoegd tussen de woorden “verbindingsgegevens of -identificatoren,” en de woorden “locatiegegevens”.
CHAPITRE 10 - Entrée en vigueur	HOOFDSTUK 10 - Inwerkingtreding
[Art. 36. La loi entre en vigueur le jour où l’annulation de la loi du 29 mai 2016 par l’arrêt n° 57/2021 de la Cour constitutionnelle prend effet.]	[Art. 36. De wet treedt in werking op de dag waarop de vernietiging van de wet van 29 mei 2016 door het arrest nr. 57/2021 van het Grondwettelijk Hof gevolgen ressorteert.]
Donné à	Gegeven te
Par le Roi :	Van Koningswege :
Le premier,	De Eerste Minister,

Alexander DE CROO	
Le Vice-Premier Ministre et Ministre des Finances, chargé de la Coordination de la lutte contre la fraude,	De Vice-eersteminister en Minister van Financiën, belast met de Coördinatie van de fraudebestrijding,
Vincent VAN PETEGHEM	
Le Vice-Premier Ministre et Ministre des Affaires sociales et de la Santé publique,	De Vice-eersteminister en Minister van Sociale Zaken en Volksgezondheid,
Frank VANDENBROUCKE	
La Vice-Première Ministre et Ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,	De Vice-eersteminister en Minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER	
Le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord,	De Vice-eersteminister en Minister van Justitie en Noordzee,
	
Vincent VAN QUICKENBORNE	
La Ministre de la Défense,	De Minister van Defensie,
Ludivine DEDONDER	
La Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique,	De Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing,

Annelies VERLINDEN	
Le secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée et de la Régie des bâtiments	De Staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy en met de Regie der gebouwen,
Mathieu MICHEL	

ROYAUME DE BELGIQUE	KONINKRIJK BELGIE
_____	_____
SERVICE PUBLIC FEDERAL X	FEDERALE OVERHEIDSDIENST X
_____	_____
Avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités	Voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten
EXPOSE DES MOTIFS	MEMORIE VAN TOELICHTING
MESDAMES ET MESSIEURS	DAMES EN HEREN,
<u>Introduction générale</u>	<u>Algemene inleiding</u>
1. <u>Arrêt de la Cour constitutionnelle du 22 avril 2021</u>	1. <u>Arrest van het Grondwettelijk Hof van 22 april 2021</u>
Le présent avant-projet de loi vise essentiellement à répondre à l'annulation par la Cour constitutionnelle dans son arrêt n° 57/2021 du 22 avril 2021 des articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques ».	Het voorliggende voorontwerp van wet beoogt in wezen tegemoet te komen aan arrest nr. 57/2021 van 22 april 2021 waarin het Grondwettelijk Hof heeft beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen.
Cette loi prévoyait l'obligation pour les fournisseurs au public de services de	Deze wet voorzag in de verplichting voor aanbieders van openbare telefoniediensten,

<p>téléphonie, en ce compris par internet, d'accès à l'Internet et de courrier électronique par Internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines catégories de données de localisation et de trafic pendant une durée de 12 mois essentiellement afin que ces données soient disponibles pour des finalités répressives et en particulier pour les enquêtes pénales. Ces données ne concernent pas le contenu des communications.</p>	<p>waaronder ook via het internet, van internettoegang, van e-mail via het internet (ongeacht of ze bij het BIPT een kennisgeving hadden gedaan of niet) om bepaalde categorieën locatie- en verkeersgegevens gedurende een periode van 12 maanden te bewaren, in hoofdzaak zodat deze gegevens beschikbaar zijn voor Law enforcement doeleinden en met name voor strafrechtelijk onderzoek. Deze gegevens hebben geen betrekking op de inhoud van de communicatie.</p>
<p>L'argumentaire de la Cour constitutionnelle renvoie à l'arrêt « Quadrature du Net » de la Cour de Justice de l'Union européenne rendu le 6 octobre 2020 (affaires C 511/18, C 512/18 et C 520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone), lequel détaille les limites à la conservation des données et suggère certaines pistes, à savoir:</p>	<p>Het betoog van het Grondwettelijk Hof verwijst naar het arrest "Quadrature du Net" van het Hof van Justitie van de Europese Unie van 6 oktober 2020 (zaken C 511/18, C 512/18 en C 520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone), waarin de grenzen van de bewaring van gegevens nader worden toegelicht en bepaalde pistes worden voorgesteld, namelijk:</p>
<p>1) La conservation généralisée et indifférenciée des données de trafic et de localisation (autres que les données d'identité civile et les adresses IP à la source de la connexion) peut uniquement être imposée aux opérateurs en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale ;</p>	<p>1) Het algemeen en ongedifferentieerd bewaren van verkeers- en locatiegegevens (met uitzondering van gegevens met betrekking tot de burgerlijke identiteit en de IP-adressen aan de bron van de verbinding) kan alleen aan exploitanten worden opgelegd in geval van een werkelijke en actuele of voorzienbare ernstige bedreiging van de nationale veiligheid;</p>
<p>2) Pour la lutte contre la criminalité grave ou la sauvegarde de la sécurité publique, seules sont permises la conservation ciblée de données, dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers, et la conservation rapide des données (« quick-freeze »), à savoir une demande de gel des données de trafic et de localisation relatives à une personne sur une courte période ;</p>	<p>2) Met het oog op het bestrijden van zware criminaliteit of het waarborgen van de openbare veiligheid zijn alleen gerichte gegevensbewaring, op bepaalde gebieden of voor bepaalde categorieën personen waarvan van tevoren is vastgesteld dat zij een bijzonder risico vormen, en snelle gegevensbewaring ("quick freeze"), d.w.z. een verzoek om verkeers- en locatiegegevens van een persoon gedurende een korte periode te bevriezen, toegestaan;</p>
<p>3) La conservation des données d'identité civile est permise pour d'autres motifs que ceux visés aux points 1) et 2), et donc notamment pour la recherche des infractions ne relevant pas de la criminalité grave ;</p>	<p>3) Het bewaren van burgerlijke-identiteitsgegevens is toegestaan om andere dan de in de punten 1) en 2) genoemde redenen, en dus met name voor het onderzoek naar strafbare feiten die niet onder de noemer ernstige criminaliteit vallen;</p>

<p>4) Seule la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale sont de nature à justifier la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion.</p>	<p>4) Enkel de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid kunnen een algemene en ongedifferentieerde bewaring rechtvaardigen van enkel de IP-adressen die zijn toegewezen aan de bron van een verbinding.</p>
<p>Dans son arrêt du 22 avril 2021, la Cour constitutionnelle indique ce qui suit : « <i>B.18. L'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué : l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours « répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi » (points 132 et 133).</i></p>	<p>In zijn arrest van 22 april 2021 zegt het Grondwettelijk Hof het volgende: "<i>B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt : de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds « beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel » (punten 132 en 133).</i>"</p>
<p>2. <u>Solutions mises en place dans la loi programme dans le cadre des possibilités laissées par la jurisprudence</u></p>	<p>2. <u>Oplossingen ingesteld in de programmawet in het kader van de mogelijkheden die door de rechtspraak worden gelaten</u></p>
<p>2.1. <u>Conservation généralisée et indifférenciée des données de trafic en cas de menace grave pour la sécurité nationale et des données d'identification</u></p>	<p>2.1. <u>Algemene en ongedifferentieerde bewaring van de verkeersgegevens in geval van ernstige bedreiging voor de nationale veiligheid en van de identificatiegegevens</u></p>
<p>Même si la Cour de Justice de l'Union européenne limite les possibilités de conservation généralisée et indifférenciée</p>	<p>Hoewel het Hof van Justitie van de Europese Unie de mogelijkheden inzake algemene en ongedifferentieerde bewaring van</p>

de données d'identification, de trafic et de localisation, cette dernière demeure possible dans certains cas de figure.	identificatie- en verkeers- en locatiegegevens beperkt, blijft zo'n bewaring mogelijk in een aantal specifieke gevallen.
<p>Ainsi, les articles 126 et 127 de la loi télécom, tels que modifiés par la présente loi, reprennent des données d'identification des utilisateurs finaux, des équipements terminaux et des services de communications électroniques (en ce compris l'adresse IP) sans viser les données de communication.</p> <p>Il convient de souligner, à cet égard, que pour se conformer à la jurisprudence précitée, les données qui doivent être conservées par les opérateurs sur la base de la nouvelle version de l'article 126 sont désormais limitées aux données d'identification. Les autres données de trafic ne doivent donc plus être conservées sur cette base.</p>	<p>Zo nemen de artikelen 126 en 127 van de telecomwet, zoals gewijzigd door de onderhavige wet, identificatiegegevens van de eindgebruikers, van de eindapparatuur en van de elektronische-communicatiediensten (waaronder ook het IP-adres) op, zonder de communicatiegegevens te beogen.</p> <p>Daarbij dient te worden onderstreept dat om zich naar de voormelde rechtspraak te schikken, de gegevens die de operatoren moeten bewaren op basis van de nieuwe versie van artikel 126 voortaan beperkt zijn tot de identificatiegegevens. De overige verkeersgegevens moeten dus niet meer op die basis worden bewaard.</p>
Une conservation généralisée et indifférenciée des données est prévue en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, conformément à ce que la Cour de justice de l'Union européenne permet. Cette menace est établie via une méthode exceptionnelle réalisée par les services de renseignement et se sécurité.	Er wordt voorzien in de algemene en ongedifferentieerde bewaring van gegevens in geval van een ernstige, werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid overeenkomstig hetgeen het Hof van Justitie van de Europese Unie toestaat. Deze dreiging wordt vastgesteld via een uitzonderlijke methode die door de inlichtingendiensten wordt uitgevoerd.
2.2. <u>Quick freeze (gel des données)</u>	2.2. <u>Quick freeze (bevriezing van de gegevens)</u>
<p>Une mesure de conservation rapide (« quick freeze ») constitue une mesure utile, dès lors qu'elle permet de prolonger la durée de conservation de certaines données.</p> <p>Cependant, une telle mesure, à elle seule, ne permet pas de lutter contre la criminalité grave et les menaces réelles et actuelles en matière de sécurité. Très concrètement, ordonner une mesure de quick freeze au moment de la détection des faits, par exemple en cas de plainte pour enlèvement ou de découverte d'un cadavre ou d'une</p>	<p>Een maatregel van snelle bewaring ("quick freeze") is een nuttige maatregel, aangezien aan de hand daarvan de duur van bewaring van bepaalde gegevens verlengd kan worden.</p> <p>Zo'n maatregel kan evenwel op zichzelf geen antwoord bieden in de strijd tegen de zware criminaliteit en de reële en actuele dreigingen op vlak van veiligheid. In wezen is het meestal al te laat als men, op het moment dat de feiten vastgesteld worden, bijvoorbeeld een ontvoering of de</p>

<p>explosion suite à un attentat est dans l'immense majorité des cas trop tard. Ce sont notamment par excellence les contacts antérieurs d'une personne qui permettent de démarrer une enquête. Cette mesure ne respecterait aucunement les droits des victimes dans la recherche de la vérité.</p> <p>Le Conseil d'Etat français, qui a été amené à examiner la législation française en matière de conservation de données de trafic pour les autorités (arrêt du 21/04/2021 nos 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), l'explique dans les termes suivants :</p>	<p>ontdekking van een lijk of bomexplosie bij een aanslag, een quick freeze beveelt. Het zijn namelijk bij uitstek de eerdere contacten van een persoon die toelaten om een onderzoek uit te diepen. De maatregel is onvoldoend om de rechten van het slachtoffer te eerbiedigen in de zoektocht naar de waarheid.</p> <p>De Franse Conseil d'Etat, die de Franse wetgeving betreffende bewaring van verkeersgegevens voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), legt dit uit in de volgende bewoording:</p>
<p><i>« 56. La conservation rapide des données de connexion est ainsi de nature à faire obstacle à la disparition des informations nécessaires à la recherche, à la constatation et à la poursuite des auteurs d'infractions pénales à compter de la date et de l'heure à laquelle il est enjoint à un opérateur d'y procéder, à la suite de la commission d'une infraction ou du recueil d'éléments donnant à penser qu'une telle infraction est projetée, ainsi qu'à l'effacement ou à l'anonymisation des données relatives à des communications antérieures lorsqu'elles ont été conservées par les opérateurs. Cependant, sur ce dernier point, l'efficacité du dispositif est subordonnée à la condition que les données aient été effectivement conservées. A défaut, la conservation rapide ne permet pas aux services d'enquête et à l'autorité judiciaire d'exploiter des données relatives aux communications effectuées avant qu'elle soit ordonnée. »</i></p>	<p><i>"56. De snelle bewaring van de connectiegegevens is aldus van die aard dat die in de weg staat van de verdwijning van de informatie die nodig is voor de opsporing, de vaststelling en de vervolging van de plegers van strafbare feiten te rekenen vanaf de datum en vanaf het tijdstip waarop een operator gelast wordt om daartoe over te gaan, na het plegen van een inbreuk of na het bundelen van elementen die doen vermoeden dat een dergelijke inbreuk gepland is, alsook van het wissen of de anonimisering van de gegevens met betrekking tot vroegere communicatie wanneer die door de operatoren zijn bewaard. Wat dat laatste punt betreft is de efficiëntie van de beschikking evenwel afhankelijk van de voorwaarde dat de gegevens daadwerkelijk zijn bewaard. Als dat niet zo is, biedt de snelle bewaring de onderzoeksdiensten en de gerechtelijke autoriteit niet de mogelijkheid om gebruik te maken van gegevens in verband met communicatie die plaatsgevonden heeft voordat die snelle bewaring bevolen is." (vrij vertaald).</i></p>
<p>Le gouvernement a opté pour créer un gel des données déjà stockées (« quick freeze ») sur des personnes qui font déjà l'objet d'une enquête, que ce soit au niveau judiciaire ou au niveau des services de renseignement et de sécurité. Ce faisant, des garanties importantes sont données au niveau des conditions de conservation puisqu'elles ne pourront s'opérer que sur demande du procureur du Roi ou du juge</p>	<p>De regering heeft gekozen voor het bevriezen van reeds opgeslagen gegevens ("quick freeze") over personen tegen wie reeds een onderzoek loopt, hetzij op het niveau van justitie, hetzij op het niveau van de inlichtingen- en veiligheidsdiensten. Daarbij worden belangrijke garanties gegeven met betrekking tot de voorwaarden van bewaring, aangezien deze alleen kunnen worden uitgevoerd op</p>

d'instruction ou, pour les services de renseignement et de sécurité, d'un chef de service et que les principes essentiels en matière d'information et d'instruction sont d'office d'application (droit de consultation du dossier, d'en prendre copie, possibilité de contester la régularité de la procédure, degré d'appel) ou pour les services de renseignement aux méthodes ordinaires.	verzoek van de procureur des Konings of de onderzoeksrechter of, in het geval van de inlichtingen- en veiligheidsdiensten, een diensthoofd, en de essentiële beginselen van informatie en onderzoek automatisch worden toegepast (recht op inzage van het dossier, recht om een kopie te nemen, mogelijkheid om de regelmatigheid van de procedure aan te vechten, mate van beroep) of, in het geval van de inlichtingendiensten, op de gewone methoden.
2.3. <u>Conservation ciblée sur base des personnes</u>	2.3. <u>Gerichte bewaring op basis van de personen</u>
Il est prévu aux articles 39quinquies du Code d'instruction criminelle et à l'article 16/2/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que les autorités judiciaires et les services de renseignement et de sécurité puissent requérir des opérateurs une conservation de données de communication ciblée sur une personne ou un groupement de personnes. Cette conservation est ponctuelle, pour une durée limitée, et axée sur la cible d'une enquête de police ou de renseignement. Cette possibilité est expliquée dans le commentaire des deux articles.	In artikel 39quinquies van het Wetboek van Strafvordering en in artikel 16/2/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst wordt bepaald dat de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten de operatoren mogen opvorderen tot het bewaren van communicatiegegevens gericht op een persoon of een groep personen. Deze bewaring is specifiek, voor een beperkte duur en gericht op het doel van een politieonderzoek of een inlichting. Die mogelijkheid wordt uitgelegd in de commentaar bij de twee artikelen.
2.4. <u>Conservation ciblée sur base géographique</u>	2.4. <u>Gerichte bewaring op geografische basis</u>
Vu l'insuffisance des données de trafic disponibles auprès des opérateurs pour répondre aux besoins des autorités, la conservation ciblée sur base géographique est mise en œuvre, en tenant compte des éléments suivants. Premièrement, la Cour de Justice de l'Union européenne a suggéré cette possibilité comme méthode de conservation admissible au regard du droit au respect de la vie privée, moyennant le recours à des critères objectifs et non discriminatoires (point 150 de l'arrêt « La Quadrature du Net »).	Gelet op de ontoereikendheid van de verkeersgegevens die beschikbaar zijn bij de operatoren om te voldoen aan de behoeften van de autoriteiten, wordt de gerichte bewaring op geografische basis toegepast, rekening houdende met de volgende elementen. Ten eerste heeft het Hof van Justitie van de Europese Unie deze mogelijkheid gesuggereerd als bewaringsmethode die toelaatbaar is ten aanzien van het recht op eerbiediging van de privacy, mits gebruik wordt gemaakt van objectieve en niet-discriminerende criteria (punt 150 van het arrest "La Quadrature du Net").

<p>Deuxièmement, il a tenu compte du fait qu'il n'est pas possible de prédire avec une certitude absolue où des faits criminels vont être commis, ni par qui.</p>	<p>Ten tweede is er rekening gehouden met het feit dat het onmogelijk is om met absolute zekerheid te voorspellen waar criminele feiten zullen plaatsvinden of door wie.</p>
<p>Dans une vision purement théorique, la conciliation parfaite des principes de vie privée et de lutte contre la criminalité grave ou de menace pour la sécurité publique implique que seules les données d'identification, de localisation et de trafic des personnes dont on a la certitude absolue qu'elles sont coupables ou victimes d'infraction pénale ou qu'elles ont besoin d'une aide ou d'une assistance pourraient être conservées. Il s'agirait de ne conserver que les seules données relatives aux auteurs d'infractions pénales qui servent à sceller la preuve de leur culpabilité et que les seules données relatives à des lieux où l'on sait avec la même assurance absolue qu'une infraction grave va être commise. Dans cette même optique purement théorique, on ne conservait alors que les données des personnes dont on sait par avance qu'elles deviendront des victimes et ce, uniquement lors de la survenance de l'infraction. Tout un chacun sait cependant qu'il n'est bien évidemment pas possible de prédéterminer d'office les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu très précis où elle sera commise.</p>	<p>Zuiver theoretisch gezien impliceert de perfecte verzoening van de beginselen van de eerbiediging van de persoonlijke levenssfeer met de bestrijding van zware criminaliteit of bedreiging van de openbare veiligheid met andere woorden dat alleen de identificatie-, locatie- en verkeersgegevens van personen van wie met absolute zekerheid bekend is dat zij schuldig zijn aan of slachtoffer zijn van strafbare feiten dan wel hulp of bijstand behoeven, mogen worden bewaard. Alleen van plegers van strafbare feiten zouden die gegevens mogen worden bewaard die strekken tot bewijs van hun schuld, en alleen de gegevens met betrekking tot locaties waarvan met dezelfde absolute zekerheid bekend is dat er een ernstig misdrijf zal worden gepleegd. In dezelfde zuiver theoretische zin worden alleen gegevens bewaard over personen van wie van tevoren bekend is dat zij slachtoffer zijn, en alleen wanneer het misdrijf plaatsvindt. Iedereen weet echter dat het uiteraard niet mogelijk is vooraf te bepalen wie betrokken zal zijn bij een strafbaar feit dat nog niet is gepleegd of waar het precies zal worden gepleegd.</p>
<p>Le gouvernement est pleinement conscient que la conservation ciblée sur base géographique entraîne inévitablement une manière totalement nouvelle pour les opérateurs de concevoir et de gérer la conservation de données de localisation et de trafic et la fourniture de ces données aux autorités. C'est dans cette optique que, pour faire face aux adaptations techniques nécessaires, les opérateurs ont reçu 3 mois pour mettre en œuvre la loi à partir de l'entrée en vigueur de l'arrêté royal qui définira les données à conserver dans le cadre de la conservation ciblée sur base géographique (article 126/1 de la loi télécom).</p>	<p>De regering is er zich ten volle van bewust dat de gerichte bewaring op geografische basis onvermijdelijk leidt tot het ontwikkelen van een totaal nieuwe manier voor de operatoren om de bewaring van locatie- en verkeersgegevens op te vatten en te beheren, alsook de verstrekking van deze gegevens aan de autoriteiten. Hierdoor wordt een periode van 3 maanden voorzien voor de operatoren om de nodige technische aanpassingen te kunnen doorvoeren, een periode die ingaat vanaf de inwerkingtreding van het koninklijk besluit dat de gegevens zal bepalen die bewaard moeten worden in het kader van de gerichte bewaring op geografische basis (artikel 126/1 van de telecomwet).</p>

Le gouvernement a également pris connaissance des difficultés techniques et opérationnelles rencontrées par les opérateurs pour mettre en œuvre la conservation ciblée sur base géographique.	De regering heeft ook kennis genomen van de technische en operationele moeilijkheden die de operatoren ondervonden om de gerichte bewaring op geografische basis te verrichten.
Il existe également un risque que les auteurs d'infraction s'organisent pour commettre des infractions dans des zones non soumises à conservation de données.	Er bestaat ook een risico dat daders van inbreuken zich organiseren om inbreuken te plegen in gebieden waar de gegevensbewaring niet van toepassing is.
Le gouvernement a en effet décidé d'opérer de la conservation de données sur des zones où il y a une menace grave pour la sécurité publique vu le taux important par 1000 habitants d'infractions graves qui s'y sont déroulées au cours des 3 années précédentes. Si ce taux est un marqueur indéniable d'une activité criminelle foisonnante, il serait absurde de ne viser que les rues, coordonnées GPS où ces infractions graves se sont tenues car cela impliquerait que les schémas criminels sont parfaitement prévisibles et se déroulent forcément aux mêmes endroits. Ici aussi, il est cependant possible de ne pas d'office cibler tout le territoire mais de regarder arrondissement par arrondissement ou zones de police par zones de police l'importance de la menace pour la sécurité publique.	De regering heeft besloten gegevens te bewaren over gebieden waar de openbare veiligheid ernstig wordt bedreigd, gezien het hoge aantal ernstige misdrijven per 1000 inwoners dat daar de afgelopen 3 jaren is gepleegd. Hoewel dit percentage een onbetwistbare indicator is van hoge niveaus van criminele activiteit, zou het absurd zijn alleen de straten en GPS-coördinaten waar deze ernstige misdrijven hebben plaatsgevonden, in het vizier te nemen, omdat dit zou impliceren dat criminele patronen volkomen voorspelbaar zijn en noodzakelijkerwijs op dezelfde plaatsen plaatsvinden. Ook hier is het echter mogelijk niet het gehele grondgebied als vanzelfsprekend te beschouwen, maar de omvang van de bedreiging van de openbare veiligheid wijk voor wijk of politiezone voor politiezone te bekijken.
Une conservation ciblée des données est prévue en cas de menace grave, réelle et actuelle pour la sécurité nationale. Cette menace est établie par l'OCAM en cas de niveau de la menace 3 ou 4.	Er wordt in een gerichte bewaring van de gegevens voorzien in geval van ernstige, reële en actuele bedreiging voor de nationale veiligheid. Deze bedreiging wordt vastgesteld door het OCAM in geval van dreigingsniveau 3 of 4.
Le gouvernement a également, comme le permet la Cour, prévu la conservation des données dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, 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 et dans les zones où il y a une menace grave potentielle pour les intérêts des institutions internationales.	De regering heeft ook, zoals toegestaan door het Hof, voorzien in de bewaring van gegevens in de zones die in het bijzonder zijn blootgesteld aan risico's van dreigingen voor de nationale veiligheid of grote risico's van zware criminaliteit, in de zones waar een mogelijke ernstige bedreiging bestaat voor de vitale belangen van de natie of voor de essentiële behoeften van de bevolking en in de zones waarin een mogelijke ernstige bedreiging bestaat voor de belangen van de internationale instellingen.

2.5. <u>Garanties auprès des opérateurs concernant l'accès aux données</u>	2.5. <u>Waarborgen bij de operatoren betreffende de toegang tot de gegevens</u>
<p>Il est bien entendu important de rappeler qu'outre les nouveaux critères et les garanties apportées au niveau de la conservation des données, les principes d'accès aux données auprès des différents opérateurs (accès uniquement sur la base du besoin d'en connaître et d'une autorisation judiciaire) restent entièrement d'application. Un croisement en masse et une vue constante et générique de l'ensemble des données d'identification, de trafic et de localisation de l'ensemble de la population tant dans le chef des services de « law enforcement » que des opérateurs constituaient et constituent dès lors des craintes absolument non fondées.</p>	<p>Er zij uiteraard aan herinnerd dat, naast de nieuwe criteria en de geboden garanties voor de bewaring van gegevens, de beginselen van toegang tot gegevens door operatoren (toegang uitsluitend op basis van het "need-to-know"-beginsel en met toestemming van de rechter), volledig van toepassing blijven. Massale kruiscontroles en een voortdurend en algemeen overzicht van alle identificatie-, verkeers- en locatiegegevens van de gehele bevolking zowel in hoofde van de "law enforcement"-diensten als van de operatoren waren en zijn derhalve volkomen ongegronde angsten.</p>
<p>Par ailleurs, la Cour de Justice de l'Union européenne insiste aussi sur la nécessité de prendre des mesures afin de prévenir les risques d'abus des données conservées . Ici aussi, il faut rappeler les mesures déjà mises en place en Belgique :</p>	<p>Bovendien wijst het Hof van Justitie van de Europese Unie ook op de noodzaak om maatregelen te nemen om de risico's van misbruik van de bewaarde gegevens te voorkomen. Ook hier moet worden herinnerd aan de maatregelen die reeds in België van kracht zijn:</p>
<p>- il y a, au sein des opérateurs, une cellule dédiée uniquement aux demandes des « law enforcement » ;</p>	<p>- Er is bij de operatoren een eenheid die zich uitsluitend bezighoudt met verzoeken om rechtshandhaving;</p>
<p>- les membres de cette cellule sont « screenés » (vérification de sécurité) avant de rejoindre cette cellule ;</p>	<p>- de leden van deze eenheid worden gescreend (veiligheidscontrole) voordat zij tot de eenheid toetreden;</p>
<p>- ces membres sont soumis au secret professionnel .</p>	<p>- deze leden zijn onderworpen aan het beroepsgeheim.</p>
<p>Afin de rencontrer les critiques de la Cour de Justice de l'Union européenne, ces mesures ont été renforcées. Concernant l'obligation pour les opérateurs de tenir un journal , la loi précise dorénavant que le journal doit être complété pour l'ensemble des traitements réalisés au profit des autorités pendant 10 ans et que ce journal, également accessible à l'IBPT et à l'Autorité de protection des données, doit être automatisé pour éviter les risques de falsification.</p>	<p>Om tegemoet te komen aan de kritiek van het Hof van Justitie van de Europese Unie zijn deze maatregelen aangescherpt. Betreffende de verplichting voor de operatoren om een logboek bij te houden schrijft de wet voortaan voor dat het logboek moet worden ingevuld voor alle verwerkingen uitgevoerd voor de autoriteiten gedurende 10 jaar en dat dit logboek, ook toegankelijk voor het BIPT en de Gegevensbeschermingsautoriteit, moet geautomatiseerd zijn om het risico van vervalsing te voorkomen</p>

2.6. <u>L'accès des autorités aux données conservées</u>	2.6. <u>De toegang van de autoriteiten tot de bewaarde gegevens</u>
<p>L'avant-projet de loi aborde également l'accès par les autorités compétentes aux données conservées. Ces autorités sont énumérées à l'article 127/1 de la loi sur les communications électroniques, qui contient la liste des catégories d'autorités qui peuvent demander l'accès aux données d'identification, de trafic et de localisation conservées par les opérateurs en vertu de ces articles au profit des autorités, des utilisateurs finaux ou pour leurs propres besoins, dans les conditions déterminées par les lois organiques de ces autorités.</p>	<p>Het voorontwerp van wet heeft ook betrekking op de toegang tot de bewaarde gegevens door de bevoegde autoriteiten. Deze autoriteiten worden opgesomd in het artikel 127/1 van de wet betreffende de elektronische communicatie, dat de lijst bevat van de categorieën van autoriteiten die toegang kunnen vragen tot de identificatie-, verkeers- en locatiegegevens, bewaard bij de operatoren krachtens deze artikelen ten behoeve van de autoriteiten, de eindgebruikers of voor hun eigen behoeften, onder de voorwaarden die bepaald worden door de organieke wetten van deze autoriteiten.</p>
<p>Cet avant-projet vise également à répondre aux attentes sociétales légitimes d'un monde de plus en plus digitalisé. En effet, force est de constater que l'e-commerce devient dans beaucoup de secteurs la norme. De la sorte, afin de lutter contre certaines formes d'infractions se commettant via le commerce en ligne, il est nécessaire que certains services d'inspection avec des pouvoirs d'enquêtes puissent disposer des données d'identification conservées par les opérateurs, afin de pouvoir démarrer une enquête. C'est dans cette optique que le service d'Inspection Produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement a, au chapitre 8, reçu la possibilité d'identifier des personnes morales ou physiques sur la base d'un numéro de téléphone ou d'une adresse IP. Il ne s'agit en d'autres termes que de données non sensibles puisqu'elles concernent des données d'identification. Dans ces hypothèses, le critère de proportionnalité est par ailleurs immédiatement rencontré vu que, sans ces accès, il y a une impossibilité matérielle pour ce service de remplir sa mission légale et que les enquêtes resteraient immuablement à charge de X. Nier cet élément factuel reviendrait</p>	<p>Met dit voorontwerp wordt tevens beoogd tegemoet te komen aan de legitieme maatschappelijke verwachtingen van een steeds meer gedigitaliseerde wereld. Het is inderdaad duidelijk dat elektronische handel in vele sectoren de norm aan het worden is. Zo is het voor de bestrijding van bepaalde vormen van strafbare feiten die via de onlinehandel worden gepleegd, noodzakelijk dat bepaalde inspectiediensten met opsporingsbevoegdheid toegang hebben tot de door de marktdeelnemers bijgehouden identificatiegegevens, zodat zij een onderzoek kunnen instellen. Met het oog hierop heeft de inspectiedienst consumentenproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, in de hoofdstuk 8, de mogelijkheid gekregen om rechtspersonen of natuurlijke personen te identificeren op basis van een telefoonnummer of IP-adres. Met andere woorden, de gegevens zijn niet gevoelig omdat zij identificatiegegevens betreffen. In deze gevallen is ook onmiddellijk voldaan aan het evenredigheids criterium, aangezien het zonder deze toegang materieel onmogelijk zou zijn voor deze dienst om zijn wettelijke taak te vervullen en de onderzoeken altijd onder de verantwoordelijkheid van X zouden blijven</p>

<p>conséquemment à créer dans internet un espace de non droit.</p>	<p>vallen. De ontkenning van dit feitelijke element zou bijgevolg neerkomen op het creëren van een rechteloze ruimte op het internet.</p>
<p>Les personnes habilitées au sein du Centre pour la Cybersécurité Belgique (CCB) reçoivent la possibilité de demander des données d'identification, de trafic et de localisation aux opérateurs dans le cadre de la prévention et de la détection des infractions en matière de cybercriminalité, de la prévention de menaces contre la sécurité publique liées à la cybersécurité ainsi que de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques.</p>	<p>De binnen het Belgisch centrum voor cyberveiligheid (CCB) gemachtigde personen krijgen de mogelijkheid om identificatie-, verkeers- en locatiegegevens op te vragen bij operatoren in het kader van het voorkomen en opsporen van misdrijven inzake cybercriminaliteit, het voorkomen van bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging en het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of –diensten.</p>
<p>Afin de mener à bien ses missions de régulateur financier et de détection et d'enquête concernant d'éventuelles infractions à la législation financière, la FSMA reçoit pour des fins de détection, l'examen et la poursuite d'abus de marché la possibilité de réaliser un quick freeze des données de trafic et de localisation. Cette mesure porte uniquement sur des données existantes qui sont encore conservées mais risquent d'être supprimées ou rendues anonymes le temps d'obtenir l'autorisation du juge d'instruction pour requérir ces données. Pour pouvoir accéder à ces données, l'auditeur de la FSMA a en effet toujours besoin de l'autorisation préalable d'un juge d'instruction. A cet égard des garanties matérielles et procédurales sont prévues. Ici aussi le principe de proportionnalité est rencontré.</p>	<p>Om haar taken als financiële toezichthouder uit te voeren en eventuele inbreuken op de financiële regelgeving op te sporen en te onderzoeken, krijgt de FSMA voor doeleinden van het opsporen, onderzoeken en vervolgen van marktmisbruik de mogelijkheid om verkeers- en locatiegegevens tijdelijk te laten "bevriezen". Deze maatregel heeft enkel betrekking op bestaande gegevens, die nog bewaard worden maar riskeren te worden verwijderd of anoniem gemaakt in afwachting van de toestemming van de onderzoeksrechter. Om toegang te krijgen tot deze gegevens heeft de auditeur van de FSMA immers steeds de voorafgaande toestemming van een onderzoeksrechter nodig. Terzake gelden de nodige materiële en procedurele waarborgen. Ook hier is voldaan aan het evenredigheidsbeginsel.</p>
<p>Pour clôturer, cet avant-projet de loi prévoit aussi quelques modifications au statut de l'IBPT. Ces modifications permettent de confirmer que l'IBPT peut demander aux opérateurs des données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions. La pratique montre en effet qu'il est parfois nécessaire que l'IBPT prenne connaissance de ces données dans le cadre de la mise en œuvre de cette loi du 13 juin 2005 ou dans le cadre du contrôle des opérateurs télécom.</p>	<p>Tot slot voorziet dit voorontwerp van wet ook in een aantal wijzigingen in het statuut van het BIPT. Dankzij deze wijzigingen kan bevestigd worden dat het BIPT van de operatoren identificatie-, verkeers- of locatiegegevens kan vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten. De praktijk toont immers aan dat het soms noodzakelijk is dat het BIPT kennis neemt van deze gegevens in het kader van de uitvoering van deze wet van 13 juni 2005 of in het kader van de controle van de telecomoperatoren.</p>

Bien entendu, dans l'ensemble de ces hypothèses, les demandes faites aux opérateurs se déroulent via la cellule de coordination de l'opérateur, ce qui implique que ces demandes d'accès font partie du journal tenu par les opérateurs et que celles-ci doivent être motivées et ciblées.	Uiteraard worden in al deze gevallen de verzoeken aan de operatoren via de coördinatiecel van de operator gedaan, hetgeen impliceert dat deze vragen om toegang deel uitmaken van het logboek dat door de operatoren wordt bijgehouden en dat zij gemotiveerd en doelgericht moeten zijn.
COMMENTAIRE DES ARTICLES	ARTIKELSGEWIJZE BESPREKING
CHAPITRE 1^{er} - Disposition générale	HOOFDSTUK 1 - Algemene bepaling
Article 1	Artikel 1
Conformément à l'article 83 de la Constitution, l'article premier précise que cet avant-projet règle des matières visées à l'article 74 de la Constitution.	Overeenkomstig artikel 83 van de Grondwet bepaalt artikel 1 dat het voorontwerp aangelegenheden regelt als bedoeld in artikel 74 van de Grondwet.
CHAPITRE 2 - Modifications à la loi du 13 juin 2005 relative aux communications électroniques	HOOFDSTUK 2 - Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie
Art. 2	Art. 2
La définition d'appels infructueux, annulée par la Cour constitutionnelle dans son arrêt du 22 avril 2021 (arrêt n°57/2021), est réintroduite dans l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques. Il convient cependant de noter que l'article 126 de cette même loi (conservation généralisée et indifférenciée de données d'identification) ne fait plus référence à la notion d'appels infructueux, qui est uniquement utilisée dans	De definitie van oproepingen zonder resultaat die het Grondwettelijk Hof had vernietigd in zijn arrest van 22 april 2021 (arrest nr. 57/2021), wordt opnieuw ingevoegd in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Er moet evenwel worden opgemerkt dat artikel 126 van diezelfde wet (algemene en ongedifferentieerde bewaring van identificatiegegevens) niet langer verwijst

l'article 126/1 (conservation ciblée sur base géographique).	naar het begrip van oproep pogingen zonder resultaat, dat enkel in artikel 126/1 wordt gebruikt (gerichte bewaring op geografische basis).
Art. 3	Art. 3
Le nouvel article 127/4 du LCE reprend l'art. 9, § 7.	Het nieuwe artikel 127/4 van de WEC neemt art. 9, § 7 over.
Art. 4	Art. 4
<u>Le paragraphe 1^{er} de l'article 122</u>	<u>Paragraaf 1 van artikel 122</u>
L'article 122, qui transpose l'article 6 de la directive « vie privée et communications électroniques » (Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques), vise les données de trafic telles que définies à l'article 2, 6°, en ce compris les données de localisation, définies à l'article 2, 7°, sauf lorsque ces données de localisation ne sont pas traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication. Dans ce cas, l'article 123 leur est applicable.	Artikel 122, die artikel 6 van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie) omzet, doelt op de verkeersgegevens zoals gedefinieerd in artikel 2, 6°, inclusief de locatiegegevens, gedefinieerd in artikel 2, 7°, behalve wanneer deze locatiegegevens niet verwerkt worden met het oog op het overbrengen van communicatie via een elektronische-communicatienetwerk of de facturering van dergelijke communicatie. In dat geval is artikel 123 daarop van toepassing.
La version antérieure de l'article 122, §1er, alinéa 2, prévoyait que l'alinéa 1er (l'obligation pour les opérateurs de supprimer les données de trafic ou de les rendre anonymes lorsqu'elles ne sont plus nécessaires pour la transmission de la communication) s'appliquait sans préjudice du respect des obligations de coopération prévues avec certaines autorités.	De vorige versie van artikel 122, § 1, tweede lid, bepaalde dat het eerste lid (de verplichting voor de operatoren om de verkeersgegevens te verwijderen of ze te anonimiseren wanneer ze niet langer nodig waren voor de transmissie van de communicatie)) gold onverminderd de naleving van de vastgelegde verplichtingen tot samenwerking met bepaalde autoriteiten.

<p>Dans un souci de clarté, la liste des autorités pouvant demander accès aux données est reprise et adaptée à l'article 127/1. Cette liste est désormais commune aux articles 122 (données de trafic), 123 (données de localisation autres que de trafic), 126 (données de souscription et données d'identité numérique), 126/1 (conservation ciblée sur base géographique) et 127 (données d'identité civile).</p>	<p>Omwille van de duidelijkheid wordt de lijst van de autoriteiten die toegang tot de gegevens kunnen vragen vermeld en aangepast in artikel 127/1. Deze lijst is voortaan gemeenschappelijk aan de artikelen 122 (verkeersgegevens), 123 (locatiegegevens die geen verkeersgegevens zijn), 126 (abonnementsgegevens en gegevens van digitale identiteit), 126/1 (doelgerichte bewaring op geografische basis) en 127 (gegevens van burgerlijke identiteit).</p>
<p><u>Le paragraphe 2 de l'article 122</u></p>	<p><u>Paragraaf 2 van artikel 122</u></p>
<p>Alors que l'ancien article 122, § 2, prévoyait une obligation pour les opérateurs de conserver des données de trafic dans le but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, cet article prévoit dorénavant une possibilité pour les opérateurs de le faire, et ce pour les raisons suivantes.</p>	<p>Terwijl het oude artikel 122, § 2, een verplichting oplegde aan de operatoren om verkeersgegevens te bewaren teneinde de abonnees te factureren of de interconnectiebetalingen uit te voeren, voorziet dit artikel voortaan in een mogelijkheid voor de operatoren om dat te doen, om de volgende redenen.</p>
<p>D'une part, une obligation n'est pas nécessaire, étant donné que les opérateurs ont tout intérêt à conserver ces données pour ces finalités et qu'il découle de l'article 110 de la présente loi, à tout le moins indirectement, que ces données doivent être disponibles. D'autre part, cette modification permet de se rapprocher de l'article 6, § 2, de la directive « vie privée et communications électroniques » (directive 2002/58/CE) que l'article 122, § 2 transpose. Cet article 6, § 2, prévoit que, par dérogation au principe de suppression ou d'anonymisation, les données de trafic peuvent être traitées à des fins de facturation.</p>	<p>Enerzijds is een verplichting niet nodig aangezien de operatoren er alle belang bij hebben om deze gegevens te bewaren voor die doeleinden en vloeit uit artikel 110 van deze wet al minstens onrechtstreeks voort dat deze gegevens beschikbaar moeten zijn. Anderzijds maakt deze wijziging het mogelijk om beter aan te sluiten bij artikel 6, § 2, van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) dat artikel 122, § 2, omzet. Dat artikel 6, § 2, bepaalt dat, in afwijking op het principe van verwijdering of anonimisering, de verkeersgegevens voor factureringsdoeleinden mogen worden gebruikt.</p>
<p>La liste des données de trafic que les opérateurs devaient traiter selon l'article 122, § 2, est supprimée, étant donné que cette liste n'est plus adaptée aux différents services de communications électroniques offerts par les opérateurs.</p>	<p>De lijst met verkeersgegevens die de operatoren dienden te behandelen volgens artikel 122, § 2, wordt geschrapt aangezien die lijst niet langer is afgestemd op de verschillende elektronische communicatiediensten die worden aangeboden door de operatoren.</p>
<p>Cette liste était surtout pertinente pour le service de téléphonie fixe et visait les données suivantes:</p>	<p>Die lijst was vooral relevant voor de vaste-telefoniedienst en beoogde de volgende gegevens:</p>

1° l'identification de la ligne appelante;	1° de identificatie van de oproeplijn;
2° les adresses relatives à l'abonné et au lieu de raccordement, ainsi que le type d'équipement terminal;	2° het adres van de abonnee en van de plaats van de aansluiting, alsook het soort eindapparatuur;
3° le nombre total d'unités à facturer pour la période de facturation;	3° het totale aantal voor de factureringsperiode aan te rekenen eenheden;
4° l'identification de la ligne appelée;	4° de identificatie van de opgeroepen lijn;
5° le type d'appel, l'heure à laquelle l'appel a commencé, la durée de l'appel ou la quantité de données transmises;	5° het type, het tijdstip van aanvang en de duur van de oproep of de verzonden hoeveelheid gegevens;
6° la date de la communication ou du service;	6° de datum van de verbinding of van de dienst;
7° d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.	7° andere gegevens betreffende de betalingen, zoals vooruitbetaling, betaling in termijnen, afsluitingen en aanmaningen.
<u>Le paragraphe 3 de l'article 122</u>	<u>Paragraaf 3 van artikel 122</u>
L'article 122, § 3, qui transpose l'article 6, § 3 de la directive « vie privée et communications électroniques » (directive 2002/58/CE), ne subit pas de modification faisant suite à l'arrêt Quadrature du Net du 6/10/2020 de la CJUE (affaires C 511/18, C 512/18 et C 520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone).	Artikel 122, § 3, die artikel 6, § 3, van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) omzet, ondergaat geen wijzigingen naar aanleiding van het arrest-Quadrature du Net van 6/10/2020 van het HvJ-EU (zaken C 511/18, C 512/18 en C 520/18: La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone).
Des modifications d'ordre légistique sont cependant opérées de manière à actualiser la référence à la réglementation en matière de protection des données à caractère personnel et à uniformiser la terminologie employée au sein des articles 122 et 123.	Wijzigingen van wetgevingstechnische aard worden evenwel doorgevoerd teneinde de verwijzing naar de reglementering inzake bescherming van persoonsgegevens bij te werken en de terminologie gebruikt in de artikelen 122 en 123 te uniformiseren.
L'article 122, § 3, 2° et 3°, est modifié pour s'aligner sur la notion de consentement au sens du RGDP (qui ne vise pas le retrait temporaire ou définitif du consentement).	Artikel 122, § 3, 2° en 3°, wordt gewijzigd om zich af te stemmen op het begrip van toestemming in de zin van de AVG (die geen tijdelijke of definitieve intrekking van de toestemming beoogt).

<u>Le paragraphe 4 de l'article 122</u>	<u>Paragraaf 4 van artikel 122</u>
<i>La définition de fraude et d'utilisation malveillante du réseau</i>	<i>De definitie van fraude en kwaadwillig gebruik van het netwerk</i>
L'article 122 définit dorénavant la notion de fraude et d'utilisation malveillante du réseau.	Artikel 122 definieert voortaan het begrip van fraude en kwaadwillig gebruik van het netwerk.
L'auteur de la fraude peut être l'utilisateur final et la victime l'opérateur (par exemple, l'utilisateur final ne respecte pas les conditions générales qui les lient à l'opérateur).	De fraudepleger kan de eindgebruiker zijn en het slachtoffer de operator (bijvoorbeeld, de eindgebruiker leeft de algemene voorwaarden niet na die hem aan de operator bindt).
L'auteur de la fraude peut aussi être un tiers, et la victime l'utilisateur final. Par exemple, un tiers fait usage d'un service de communications électroniques au nom de l'abonné à son insu, le harponnage par SMS (« smishing »), le harponnage par Internet (« phishing ») ou encore un appel entrant induisant l'utilisateur final en erreur sur l'origine de cet appel et lui causant un préjudice (« spoofing »).	De fraudepleger kan ook een derde zijn, en het slachtoffer de eindgebruiker. Bijvoorbeeld, een derde maakt gebruik van een elektronische-communicatiedienst op naam van de abonnee buiten zijn medeweten, phishing via sms ("smishing"), phishing of een binnenkomende oproep die de eindgebruiker misleidt wat de oorsprong van deze oproep betreft en hem daarbij nadeel berokkent ("spoofing").
L'utilisation malveillante du réseau couvre par exemple le harcèlement par téléphone.	Kwaadwillig gebruik van het netwerk dekt bijvoorbeeld pesterijen via de telefoon.
<i>Le cadre de l'Union européenne</i>	<i>Het kader van de Europese Unie</i>
Le traitement et la conservation des données de trafic pour protéger les intérêts de l'opérateur et de l'utilisateur final contre la fraude et l'utilisation malveillante du réseau entrent dans les limites permises par la directive « vie privée et communications électroniques » (directive 2002/58/CE).	De verwerking en de bewaring van verkeersgegevens om de belangen van de operator en de eindgebruiker te vrijwaren van fraude en kwaadwillig gebruik van het netwerk vallen binnen de door de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) toegestane limieten.
En effet, l'article 6, § 5, de la directive « vie privée et communications électroniques » énonce que « Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées [...] de détecter les	Artikel 6, § 5, van de Richtlijn betreffende privacy en elektronische communicatie stelt immers dat "De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor [...] opsporing van fraude [...], en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren."

<p>fraudes [...] ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités. »</p>	
<p>En outre, l'article 15, §1er, de la même directive prévoit que les États membres peuvent déroger aux règles prévues par son article 6 lorsque cela constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour la poursuite de l'une des finalités énumérées à cet article 15, §1er.</p>	<p>Bovendien stelt artikel 15, § 1, van dezelfde richtlijn dat de lidstaten kunnen afwijken van de regels vastgelegd in haar artikel 6 wanneer dat een noodzakelijke, gepaste en evenredige maatregel betreft, binnen een democratische maatschappij, ter nastreving van een van de doeleinden opgelijst in dit artikel 15, § 1.</p>
<p>Parmi ces finalités figurent la sauvegarde de la sécurité nationale, la protection de la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales, au sujet desquelles la Cour de justice de l'Union européenne (CJUE) s'est prononcée dans le cadre de l'arrêt La Quadrature du Net (aff. jtes. C-511/18, C-512/18 et C-520/18, du 6 octobre 2020).</p>	<p>Deze doeleinden omhelzen de vrijwaring van de nationale veiligheid, de bescherming van de openbare veiligheid, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, waarover het Europees Hof van Justitie zich heeft uitgesproken in het kader van het arrest-La Quadrature du Net (gevoegde zaken C-511/18, C-512/18 en C-520/18, van 6 oktober 2020).</p>
<p>D'autres finalités, sur lesquelles la CJUE ne s'est pas prononcée à ce stade, sont également permises par l'article 15, §1er de la directive. Il s'agit, en particulier, de la prévention, la recherche, la détection d'utilisations non autorisées du système de communications électroniques et des motifs d'exception prévus à l'article 13 de la directive 95/46, remplacé par l'article 23, §1er du RGPD (cf. arrêt de la CJUE du 29 janvier 2008, Promusicae, C-275/06, pt. 53), parmi lesquels figurent les autres objectifs importants d'intérêt public général (art. 23, §1er e) du RGPD) et la protection de la personne concernée ou des droits et libertés d'autrui (art. 23, §1er g) du RGPD).</p>	<p>Andere doeleinden, waarover het HvJ-EU zich in dit stadium niet heeft uitgesproken, worden eveneens toegestaan door artikel 15, § 1, van de richtlijn. Het gaat met name om de voorkoming, het onderzoek en de opsporing van niet-toegestaan gebruik van het elektronische-communicatiesysteem en om de uitzonderingsredenen vastgelegd in artikel 13 van Richtlijn 95/46, vervangen door artikel 23, § 1, van de AVG (cf. arrest van het HvJ-EU van 29 januari 2008, Promusicae, C-275/06, pt. 53), waaronder de andere belangrijke doelstellingen van algemeen belang (art. 23, § 1, e) van de AVG) en de bescherming van de betrokken persoon of de rechten en vrijheden van anderen (art. 23, § 1, g) van de AVG).</p>
<p>La protection de l'intérêt de l'utilisateur à disposer d'un service de communication électronique de qualité, exempt de nuisances frauduleuses, entre également dans ce cadre.</p>	<p>Ook de bescherming van het belang van de gebruiker om te beschikken over een kwalitatieve elektronische-communicatiedienst, vrij van frauduleuze hinder, valt binnen dat kader.</p>
<p>Finalement, la finalité de lutte contre la fraude et l'utilisation malveillante du réseau figure parmi les objectifs expressément prévus par le projet européen de règlement ePrivacy, voué à remplacer la directive « vie privée et</p>	<p>Ten slotte behoort de bestrijding van fraude en kwaadwillig gebruik van het netwerk tot de doelstellingen die uitdrukkelijk zijn geformuleerd in het ontwerp van de ePrivacy-verordening, dat bestemd is om de richtlijn betreffende privacy en elektronische</p>

communications électroniques » (directive 2002/58/CE).	communicatie te vervangen (Richtlijn 2002/58/EG).
Une modernisation de la présente loi, tenant compte de l'importance croissante de cet objectif, est donc souhaitable.	Het is dus wenselijk om deze wet te updaten, rekening houdend met het toenemende belang van deze doelstelling.
<i>L'obligation pour les opérateurs de traiter et conserver les données de trafic</i>	<i>De verplichting voor de operatoren om de verkeersgegevens te bewaren en te verwerken</i>
Dans la version actuelle de l'article 122, § 4, les opérateurs disposent de la possibilité de traiter des données de trafic afin de déceler des fraudes éventuelles. Il convient d'obliger les opérateurs à le faire pour les raisons suivantes.	In de huidige versie van artikel 122, § 4, beschikken de operatoren over de mogelijkheid om verkeersgegevens te verwerken om eventuele fraude op te sporen. Het is zaak om de operatoren daartoe te verplichten om de volgende redenen.
Une possibilité pour l'opérateur de traiter les données de trafic en matière de fraude implique qu'un opérateur pourrait décider de ne pas le faire (parce que la fraude ne lui cause pas de préjudice financier), ce qui pourrait porter atteinte aux intérêts de l'utilisateur final. Il convient à cet égard de veiller à ce que les opérateurs offrent un service de qualité à leurs abonnés, sans se contenter de simplement permettre une communication électronique.	De mogelijkheid voor de operator om de verkeersgegevens te verwerken in het kader van fraude houdt in dat een operator zou kunnen beslissen om dat niet te doen (omdat de fraude hem geen financieel nadeel berokkent), hetgeen de belangen van de eindgebruiker zou kunnen schaden. In dat opzicht dient ervoor te worden gezorgd dat de operatoren een kwalitatieve dienst bieden aan hun abonnees, zonder genoeg te nemen met enkel het mogelijk maken van elektronische communicatie.
Cette possibilité implique également que de grandes différences peuvent exister entre opérateurs, certains étant plus actifs que d'autres dans la protection des intérêts des utilisateurs finaux en matière de fraude.	Deze mogelijkheid houdt ook in dat er grotere verschillen kunnen bestaan tussen operatoren, aangezien sommigen actiever zijn dan anderen wat betreft de bescherming van de belangen van de eindgebruikers op het stuk van fraude.
Il convient aussi de prendre en compte la multiplication des fraudes, leur impact pour les utilisateurs finaux et le fait que c'est de plus en plus souvent l'utilisateur final et non plus l'opérateur qui est victime de la fraude.	Er dient ook rekening te worden gehouden met het toenemende aantal fraudegevallen, de impact daarvan op de eindgebruikers en het feit dat het steeds vaker de eindgebruiker is en niet de operator die het slachtoffer is van de fraude.
Bien entendu, dans certains cas, il ne sera pas techniquement possible pour les opérateurs de détecter certaines fraudes ou certaines utilisations malveillantes du réseau ou de contribuer à en établir leur existence avec les seuls données de trafic, par exemple si cette opération nécessite de prendre	In bepaalde gevallen zal het uiteraard technisch niet mogelijk zijn voor de operatoren om bepaalde gevallen van fraude of vormen van kwaadwillig gebruik van het netwerk op te sporen of bij te dragen tot de vaststelling daarvan aan de hand van enkel de verkeersgegevens, bijvoorbeeld wanneer

connaissance du contenu des communications (par exemple le contenu d'un SMS), ce que l'article 122 ne permet pas. Par ailleurs, dans certains cas, l'opérateur peut seulement disposer d'indices qu'il s'agit d'une fraude potentielle ou d'une utilisation malveillante potentielle du réseau, sans disposer de certitude à cet égard.	voor deze handeling kennis moet worden genomen van de inhoud van de communicatie (bijvoorbeeld de inhoud van een sms), wat artikel 122 niet toestaat. In sommige gevallen beschikt de operator overigens misschien enkel over aanwijzingen dat het gaat om mogelijke fraude of mogelijk kwaadwillig gebruik van het netwerk, zonder daar zeker van te zijn.
Cependant, il est essentiel que les opérateurs développent les outils et l'expertise nécessaire en matière de détection de fraude, qu'ils analysent les fraudes et comprennent leur origine et qu'ils prennent les actions adéquates sur base de cette analyse.	Toch is het van essentieel belang dat de operatoren de nodige tools en expertise inzake de opsporing van fraude ontwikkelen, dat ze de fraudegevallen analyseren en de herkomst ervan begrijpen en dat ze de passende acties ondernemen op basis van deze analyse.
D'autres données que les données de facturation peuvent être nécessaires pour détecter ou analyser la fraude ou l'utilisation malveillante du réseau, par exemple les données de localisation de l'appelant et les données liées aux communications entrantes, telles que les SMS et appels entrants.	Er kunnen ook andere gegevens dan de factureringsgegevens nodig zijn om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, bijvoorbeeld de locatiegegevens van de beller en de gegevens in verband met de binnenkomende communicatie, zoals sms'en en inkomende oproepen.
La facturation ne permet pas, par exemple, de mettre en évidence un SMS entrant, qui constitue un smishing, et le gain obtenu par le fraudeur ne se reflètera pas nécessairement dans un appel sortant.	De facturering maakt het bijvoorbeeld niet mogelijk om een binnenkomende sms die smishing vormt te doen uitkomen en de winst die de fraudeur behaalt, zal niet noodzakelijk weerspiegeld worden in een uitgaande oproep.
La facturation ne permet généralement pas de contribuer à établir le harcèlement par téléphone (les appels entrants ne sont pas facturés).	Het is doorgaans niet mogelijk om aan de hand van de facturering bij te dragen tot de vaststelling van pesterijen via de telefoon (binnenkomende oproepen worden niet gefactureerd).
La facturation ne permet pas non plus de retracer la localisation de l'équipement terminal employé pour réaliser une fraude, alors que cette localisation peut être pertinente pour détecter la fraude (différentes localisations peuvent par exemple s'avérer être incohérentes ou suspectes) et pour l'analyser.	De facturering maakt het evenmin mogelijk om de locatie te achterhalen van de eindapparatuur gebruikt om de fraude te plegen, terwijl deze plaatsbepaling relevant kan zijn om de fraude op te sporen (verschillende locaties kunnen bijvoorbeeld incoherent of verdacht blijken) en te analyseren.
Il convient d'éviter que les opérateurs décident de conserver les données de trafic pendant un laps de temps trop court que pour	Er moet worden vermeden dat de operatoren beslissen om de verkeersgegevens te bewaren voor een periode die te kort is om

<p>pouvoir efficacement lutter contre les fraudes ou que les pratiques des différents opérateurs divergent fortement. Dès lors, l'article 122 prévoit dorénavant une durée minimale de conservation de données. Dans bien des cas, l'opérateur ne pourra pas détecter la fraude ou l'utilisation malveillante du réseau lorsque la communication a eu lieu. Cependant, il est possible qu'il en soit informé ultérieurement (par exemple en cas de plainte de l'abonné auprès de l'opérateur). L'opérateur doit encore disposer de suffisamment de données de trafic (en ce compris des données de localisation) pour l'ensemble de ses abonnés pour pouvoir analyser la communication à l'origine de la fraude ou de l'utilisation malveillante du réseau.</p>	<p>fraude efficiënt te kunnen bestrijden of dat de praktijken van de verschillende operatoren sterk uiteenlopen. Vandaar dat artikel 122 voortaan in een minimale duur voor gegevensbewaring voorziet. In heel wat gevallen zal de operator de fraude of het kwaadwillig gebruik van het netwerk niet kunnen opsporen, wanneer de communicatie heeft plaatsgevonden. Het is evenwel mogelijk dat hij daar later van op de hoogte wordt gebracht (bijvoorbeeld in geval van een klacht van de abonnee bij de operator). De operator moet nog over voldoende verkeersgegevens beschikken (waaronder locatiegegevens) voor al zijn abonnees om de communicatie te kunnen analyseren die aan de oorsprong ligt van de fraude of het kwaadwillig gebruik van het netwerk.</p>
<p>Le délai de quatre mois a été retenu pour l'application de l'alinéa 3, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné).</p>	<p>De termijn van vier maanden is in aanmerking genomen voor de toepassing van het derde lid, aangezien de fraude een impact kan hebben op de facturering van de operator tegenover de abonnee (of van een onderneming tegenover de abonnee).</p>
<p>Le délai minimal de quatre mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard possible dans ce traitement (le quatrième mois suivant la consommation).</p>	<p>De minimale termijn van vier maanden bewaring houdt rekening met een volledige factureringscyclus (eerste maand volgend op het verbruik van de dienst), met een minimale duur voor betwisting (van 15 dagen tot 1 maand, de tweede maand volgend op het verbruik van de dienst), met een periode voor de behandeling van de betwisting die een uitwisseling tussen de abonnee en de operator mogelijk maakt (de derde maand volgend op de betwisting van de dienst) en met een periode van mogelijke vertraging in die behandeling (de vierde maand volgend op het verbruik).</p>
<p>Le délai de 4 mois permettra aussi de prendre en compte les évolutions en matière de fraude.</p>	<p>De termijn van 4 maanden zal het ook mogelijk maken om rekening te houden met de ontwikkelingen op het stuk van fraude.</p>
<p>Pour détecter et analyser une fraude ou une utilisation malveillante du réseau, les opérateurs sont amenés à traiter les données de trafic en temps réel et les données de trafic conservées sur base du paragraphe 2 (les données de trafic conservées dans le but d'établir les factures des abonnés ou</p>	<p>Om fraude of kwaadwillig gebruik van het netwerk op te sporen en te analyseren, dienen de operatoren de verkeersgegevens in real time te verwerken alsook de gegevens bewaard krachtens paragraaf 2 (de verkeersgegevens bewaard voor doeleinden van facturering van de abonnees of om de</p>

d'effectuer les paiements d'interconnexion) et du présent paragraphe.	interconnectiebetalingen uit te voeren) en krachtens deze paragraaf.
Lorsque l'opérateur a détecté une fraude potentielle ou avérée envers son abonné, il lui revient de prendre les mesures les plus appropriées pour protéger son abonné. Une de ces mesures peut être l'information de ce dernier, par exemple l'information que l'appel pourrait être frauduleux.	Wanneer de operator een mogelijk of bewezen geval van fraude heeft opgespoord jegens zijn abonnee, dient hij de meest gepaste maatregelen te nemen om zijn abonnee te beschermen. Een van die maatregelen kan bestaan in het informeren van deze laatste, bijvoorbeeld hem melden dat de oproep frauduleus kan zijn.
Par ailleurs, les opérateurs doivent pouvoir contribuer à établir une utilisation malveillante du réseau (par exemple en confirmant qu'une certaine communication entrante a bien eu lieu dans le cadre d'une plainte d'harcèlement par téléphone).	Verder moeten de operatoren kunnen bijdragen tot het vaststellen van kwaadwillig gebruik van het netwerk (bijvoorbeeld door te bevestigen dat er wel degelijk een zekere communicatie is binnengekomen in het kader van een klacht in verband met telefonische pesterijen).
En pratique, en cas de harcèlement par téléphone, la victime doit s'adresser au service de médiation pour les télécommunications.	In geval van telefonische pesterijen moet het slachtoffer zich in de praktijk richten tot de Ombudsdienst voor telecomcommunicatie.
Ce dernier, qui a pour mission l'aide aux victimes et n'est pas rattaché à un service de police, pourra alors obtenir via les opérateurs concernés les nom, prénom et adresse de l'auteur du harcèlement par téléphone et pourra fournir ces données à la victime de ce harcèlement (voir article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques). En pratique, un délai de conservation des données inférieur à 12 mois serait problématique, au vu des différentes étapes susmentionnés à suivre. Il convient également de souligner que le harcèlement par téléphone n'aura pas d'impact sur la facturation de l'opérateur à l'abonné, étant donné qu'il s'agit de communications entrantes.	Deze laatste, die als opdracht heeft hulp te verlenen aan de slachtoffers en die niet onder een politiedienst valt, zal dan via de betrokken operatoren de naam, voornaam en het adres van de dader van de telefonische pesterijen kunnen krijgen en zal deze gegevens kunnen verstrekken aan het slachtoffer van die pesterijen (zie artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven). In de praktijk zou een termijn van gegevensbewaring van minder dan 12 maanden problematisch zijn gezien de verschillende voormelde stappen die moeten worden gevolgd. Er dient ook te worden benadrukt dat de telefonische pesterijen geen impact zullen hebben op de facturering van de operator aan de abonnee, aangezien het om binnenkomende communicatie gaat.
<i>L'arrêté royal</i>	<i>Het koninklijk besluit</i>
La délégation au Roi introduite dans le paragraphe 4 permet de préciser dans un arrêté royal les obligations des opérateurs en	Dankzij de delegatie aan de Koning die ingevoerd is in de vierde paragraaf kunnen in een koninklijk besluit de verplichtingen van de operatoren worden verduidelijkt inzake

matière de lutte contre la fraude ou l'utilisation malveillante du réseau.	bestrijding van fraude of kwaadwillig gebruik van het netwerk.
L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaître ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour. Ensuite, les données que les opérateurs conservent pour lutter contre les fraudes peuvent être différentes selon le type de service de communications électroniques fourni, la taille de l'opérateur et les outils « anti-fraude » dont il dispose ou le type d'utilisateurs du service.	De aanneming van dit koninklijk besluit is niet verplicht in het licht van de volgende uitdagingen. Ten eerste evolueert fraude aanzienlijk mettertijd. Bepaalde vormen van fraude kunnen verdwijnen of minder belangrijk worden terwijl nieuwe soorten van fraude kunnen opduiken. Vervolgens kunnen de gegevens die de operatoren bewaren om fraude tegen te gaan, verschillen afhankelijk van het type van de verstrekte elektronische-communicatiedienst, de omvang van de operator en de "antifraudetools" waarover hij beschikt of het soort van gebruikers van de dienst.
De plus, les actions que l'opérateur prend lorsqu'il détecte une fraude potentielle ou avérée peuvent être diverses en fonction du type de fraude et du degré de certitude que l'opérateur a par rapport au fait qu'il s'agit bien d'une fraude (seulement des indices ou une certitude à cet égard).	Bovendien kunnen de acties die de operator onderneemt wanneer hij een mogelijk of bewezen geval van fraude heeft opgespoord, variëren naargelang van het type van fraude en van de graad van zekerheid die de operator heeft ten opzichte van het feit dat het wel degelijk om fraude gaat (enkel aanwijzingen of een zekerheid wat dat betreft).
La pratique devra donc être évaluée pour déterminer si un tel arrêté royal est nécessaire.	De praktijk zal dus moeten worden geëvalueerd om vast te stellen of een dergelijk koninklijk besluit noodzakelijk is.
<i>La communication des données aux autorités</i>	<i>Het bezorgen van de gegevens aan de autoriteiten</i>
Pour que les autorités compétentes (les autorités judiciaires, les services de police, les officiers de police judiciaire de l'IBPT, etc.) puissent investiguer une fraude ou une utilisation malveillante d'un réseau et retrouver l'auteur de cette fraude ou de cette utilisation malveillante, il est nécessaire qu'ils reçoivent de l'opérateur les données de trafic y afférentes.	Opdat de bevoegde autoriteiten (de gerechtelijke autoriteiten, de politiediensten, de officiers van gerechtelijke politie van het BIPT, enz. een geval van fraude of een kwaadwillig gebruik van een netwerk kunnen onderzoeken, en de pleger van deze fraude of dit kwaadwillig gebruik kunnen terugvinden, moeten zij vanwege de operator de desbetreffende verkeersgegevens ontvangen.
Le mot « présumé » est ajouté puisque les autorités doivent d'abord avoir connaissance de l'infraction potentielle avant de pouvoir mener leur enquête visant à établir l'existence d'un délit.	Het woord "vermoed" wordt toegevoegd aangezien de autoriteiten eerst kennis moeten hebben van de potentiële inbreuk, voordat ze hun onderzoek kunnen voeren om het bestaan van een wanbedrijf vast te stellen.

<u>Le paragraphe 4/1 de l'article 122</u>	<u>Paragraaf 4/1 van artikel 122</u>
<i>Introduction</i>	<i>Inleiding</i>
Le paragraphe 4/1 est introduit vu que les données de trafic peuvent contribuer à la sécurité des réseaux, qu'il est essentiel d'assurer.	Paragraaf 4/1 wordt ingevoerd, aangezien de verkeersgegevens kunnen bijdragen tot de veiligheid van de netwerken, waarvan het van fundamenteel belang is dat die gewaarborgd is.
Une obligation de traiter et conserver les données de trafic pour la finalité de sécurité des réseaux se justifie comme suit.	Een verplichting om de verkeersgegevens ten behoeve van netwerkveiligheid te verwerken en bewaren, is als volgt te rechtvaardigen.
En vertu de la loi télécom, les opérateurs doivent prendre les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement en ce qui concerne la sécurité du réseau. Cette obligation implique le traitement et la conservation de données de trafic nécessaires à cet égard.	Krachtens de telecomwet moeten de operatoren de passende technische en organisatorische maatregelen treffen om de risico's voor de veiligheid van hun netwerken of diensten op gepaste wijze te beheersen, eventueel samen wat de netwerkveiligheid betreft. Die verplichting houdt de verwerking en bewaring van de daartoe noodzakelijke gegevens in.
L'article 2, 21, de la directive (UE) 2018/172 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen définit la sécurité des réseaux et des services comme suit : « la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services ».	Artikel 2, 21°, van Richtlijn (EU) 2018/172 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie definieert de beveiliging van netwerken en diensten als volgt: "het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van die netwerken en diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronische-communicatienetwerken en -diensten worden aangeboden, in gevaar brengen".
Une obligation permet également une uniformisation des pratiques entre les opérateurs.	Aan de hand van een verplichting kunnen ook de praktijken tussen de operatoren geüniformeerd worden.
Finalement, la sécurité des réseaux, qui se rattache à la sécurité publique, est essentielle	Ten slotte is netwerkveiligheid, wat onder staatsveiligheid valt, essentieel voor de

pour la société dans son ensemble. Un incident au niveau du réseau d'un opérateur peut avoir des conséquences très dommageables sur de nombreux plans (vol ou perte de données, impact sur tous les services qui sont offerts à l'aide du réseau). L'importance de la sécurité des réseaux va croître dans le futur avec le développement de la 5G, dont seront dépendants de nombreux services et applications.	maatschappij in haar geheel. Een incident op het netwerk van een operator kan erg schadelijke gevolgen hebben op tal van niveaus (diefstal of verlies van gegevens, impact op de diensten die worden aangeboden via het netwerk). Het belang van netwerkveiligheid zal toenemen in de toekomst met de ontwikkeling van 5G, waarvan tal van diensten en applicaties zullen afhangen.
<i>Cadre de l'Union européenne</i>	<i>Het kader van de Europese Unie</i>
À nouveau, cette finalité figure parmi les motifs de traitement admissibles au regard de la directive « vie privée et communications électroniques » (directive 2002/58/CE). En effet, le considérant 29 de la directive « vie privée et communications électroniques » (directive 2002/58/CE) prévoit que : « Au besoin, et au cas par cas, le fournisseur d'un service peut traiter des données relatives au trafic qui concernent des abonnés ou des utilisateurs s'il s'agit de déceler une défaillance technique ou une erreur dans la transmission des communications. »	Ook dit doeleinde is opgenomen in de toegestane redenen voor verwerking in het licht van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG). Considerans 29 van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) bepaalt het volgende: "De dienstenaanbieder mag zo nodig in individuele gevallen verkeersgegevens met betrekking tot abonnees en gebruikers verwerken om technische defecten of fouten in de transmissie van communicatie op te sporen."
En outre, la sécurité des réseaux figure également parmi les dérogations nationales permises en vertu de l'article 15, §1er de la même directive (cf. arrêt de la CJUE du 29 janvier 2008, Promusicae, C-275/06, pt. 52).	Bovendien behoort ook de beveiliging van de netwerken tot de toegestane nationale afwijkingen krachtens artikel 15, § 1, van dezelfde richtlijn (cf. arrest van het HvJ-EU van 29 januari 2008, Promusicae, C-275/06, pt. 52).
Pour le surplus, cette finalité est également reprise expressément parmi les motifs permettant le traitement de données de trafic par les opérateurs à l'article 6, §1er du projet de règlement ePrivacy (voué à remplacer la directive précitée).	Wat het overige betreft, is dit doeleinde eveneens uitdrukkelijk opgenomen in de redenen die de operatoren toestaan om verkeersgegevens te verwerken in artikel 6, § 1, van het ontwerp van ePrivacy-verordening (die de voormelde richtlijn zal vervangen).
De même qu'indiqué précédemment pour ce qui concerne la lutte contre la fraude et l'utilisation malveillante du réseau, de manière à moderniser la présente loi et à tenir compte de l'importance croissante de l'objectif de protection de la sécurité et du bon fonctionnement des réseaux et services de communications électroniques des opérateurs, il est souhaitable d'inclure expressément cet objectif comme finalité	Zoals eerder aangegeven op het stuk van bestrijding van fraude en kwaadwillig gebruik van het netwerk, is het wenselijk, teneinde deze wet te updaten en rekening te houden met het toenemende belang van het doel bestaande in de vrijwaring van de veiligheid en de goede werking van de elektronische-communicatienetwerken en -diensten van de operatoren, om dit doel uitdrukkelijk op te nemen als reden voor de bewaring en verwerking van verkeersgegevens.

justifiant la conservation et le traitement de données de trafic.	
<i>L'obligation de conserver et traiter des données de trafic en vue de la sécurité du réseau</i>	<i>De verplichting om verkeersgegevens te bewaren en om te verwerken met het oog op netwerkveiligheid</i>
L'analyse d'une attaque (potentielle) envers le réseau n'est pas possible sans données de trafic.	Een (potentiële) aanslag op het netwerk analyseren, is niet mogelijk zonder verkeersgegevens.
Il n'est pas toujours possible pour l'opérateur de retrouver l'attaquant, de pouvoir l'identifier et de localiser l'origine de l'attaque sur base des données de trafic, étant donné que certaines attaques peuvent être très sophistiquées.	Het is voor een operator niet altijd mogelijk om de aanvaller te vinden, om deze te identificeren en de herkomst van de aanval te lokaliseren aan de hand van verkeersgegevens aangezien bepaalde aanvallen erg gesofisticeerd kunnen zijn.
Cependant, l'opérateur doit conserver les données de trafic pertinentes pour augmenter la probabilité d'y arriver.	Toch moet de operator de relevante verkeersgegevens bewaren om de slaagkansen daarvan te vergroten.
Le paragraphe 4/1 oblige les opérateurs à exploiter les données de trafic mais uniquement lorsque c'est nécessaire pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques. Dans ce cas, seules les données de trafic nécessaires à cette fin peuvent être exploitées.	Paragraaf 4/1 verplicht de operatoren om verkeersgegevens te benutten maar enkel wanneer dat nodig is om de veiligheid en correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen. In dat geval mogen enkel de daartoe noodzakelijke verkeersgegevens worden benut.
Les opérateurs peuvent par exemple exploiter des données de trafic en temps réel ou des données de trafic conservées pour rechercher les attaques sur le réseau ou pour investiguer une attaque (potentielle) sur le réseau.	De operatoren mogen bijvoorbeeld verkeersgegevens in real time of bewaarde verkeersgegevens benutten om de aanvallen op het netwerk te zoeken of om een (mogelijke) aanval op het netwerk te onderzoeken.
Cette disposition n'oblige pas les opérateurs à exploiter l'ensemble des données de trafic par défaut.	Deze bepaling verplicht de operatoren niet om automatisch alle verkeersgegevens te benutten.
La pratique montre qu'une attaque envers le réseau d'un opérateur peut être hautement sophistiquée et qu'il est possible que l'opérateur ne détecte une intrusion dans son réseau qu'après un certain laps de temps. Dès lors, il est nécessaire que l'opérateur puisse remonter suffisamment de temps dans le passé, une intrusion dans le réseau pouvant mener à une perte ou à un vol de	De praktijk leert ons dat een aanval op het netwerk van een operator heel ingewikkeld kan zijn en dat het mogelijk is dat de operator een indringing in zijn netwerk pas na verloop van enige tijd ontdekt. Vandaar dat het nodig is dat de operator voldoende kan terugkeren in de tijd, omdat een indringing in het netwerk kan leiden tot een verlies of een diefstal van gegevens. Om te kunnen terugkeren in het

données. Pour pouvoir remonter dans le passé, il est nécessaire que des données de trafic aient été conservées.	verleden, is het nodig dat de verkeersgegevens werden bewaard.
<u>Le paragraphe 4/2 de l'article 122</u>	<u>Paragraaf 4/2 van artikel 122</u>
Un opérateur doit pouvoir conserver des données de trafic pour répondre à ses obligations légales, comme par exemple la législation comptable ou fiscale ou pour répondre à une injonction d'une autorité de geler les données (également connu comme le « quick freeze »), qui se trouve par exemple dans le Code d'instruction criminelle. Ces obligations légales ne ressortent pas du présent paragraphe mais bien des législations spécifiques qui les prévoient. Cette disposition permet également de tenir compte des évolutions futures (nouvelles obligations).	Een operator moet verkeersgegevens kunnen bewaren om te voldoen aan zijn wettelijke verplichtingen, bijvoorbeeld de boekhoudkundige of fiscale wetgeving of om te voldoen aan een bevel vanwege een autoriteit om de gegevens te bevriezen (ook bekend onder de naam "quick freeze"), wat bijvoorbeeld vervat is in het Wetboek van Strafvordering. Deze wettelijke verplichtingen vloeien niet voort uit deze paragraaf maar wel degelijk uit specifieke wetgevingen die daarin voorzien. Deze bepaling maakt het ook mogelijk om rekening te houden met de toekomstige ontwikkelingen (nieuwe verplichtingen).
Conformément à l'article 15, §1er de la directive « vie privée et communications électroniques » (directive 2002/58/CE), toute obligation légale de conservation de données de trafic doit être nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour atteindre la finalité poursuivie, et adoptée dans le respect des principes généraux du droit européen, en ce compris ceux visés par la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme.	Conform artikel 15, § 1, van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG), moet elke wettelijke verplichting tot bewaring van verkeersgegevens in een democratische samenleving noodzakelijk, redelijk en proportioneel zijn, om het streefdoel te bereiken, en aangenomen worden met naleving van de algemene beginselen van het Europees recht, waaronder diegene die beoogd worden in het Handvest van de grondrechten van de Europese Unie en in het Europese Verdrag tot bescherming van de rechten van de mens.
<u>Le paragraphe 5 de l'article 122</u>	<u>Paragraaf 5 van artikel 122</u>
Les modifications au paragraphe 5 sont nécessaires pour tenir compte des nouveaux paragraphes 4/1 et 4/2 de l'article 122. Par ailleurs, la cellule de coordination de l'opérateur est chargée de fournir à une autorité les données de trafic qu'elle demande.	De wijzigingen in paragraaf 5 zijn noodzakelijk om rekening te houden met de nieuwe paragrafen 4/1 en 4/2 van artikel 122. Bovendien is de coördinatiecel van de operator ermee belast aan een autoriteit de verkeersgegevens te verstrekken die zij vraagt.
<u>Le paragraphe 6 de l'article 122</u>	<u>Paragraaf 6 van artikel 122</u>
Le Médiateur télécom a été ajouté aux autorités qui peuvent être informées des	De Ombudsman voor telecom is toegevoegd aan de autoriteiten die ingelicht kunnen

données de trafic et de facture pertinentes en vue du règlement de litiges.	worden over de relevante verkeers- en factuurgegevens met het oog op geschillenbeslechting.
Cet ajout clarifie la possibilité pour l'opérateur de transmettre des données de trafic au Médiateur télécom lorsqu'une plainte introduite à son encontre est introduite auprès de ce service.	Deze toevoeging verduidelijkt de mogelijkheid voor de operator om verkeersgegevens door te sturen naar de Ombudsman voor telecom wanneer bij die dienst tegen deze operator een klacht is ingediend.
La présente disposition ne confère cependant pas de compétences nouvelles au Médiateur télécom.	Deze bepaling kent echter geen nieuwe bevoegdheden toe aan de Ombudsdienst voor telecom.
<u>Le paragraphe 7 de l'article 122</u>	<u>Paragraaf 7 van artikel 122</u>
Afin d'écarter toute ambiguïté potentielle, il est précisé que le présent article 122 se comprend sans préjudice de l'article 127/1. En effet, la conservation et les autres types de traitements autorisés dans le chef des opérateurs sur le pied de l'article 122 n'excluent pas l'obligation pour les opérateurs de faire droit aux demandes d'accès des autorités formulées conformément à l'article 127/1 de la présente loi.	Om alle mogelijke onduidelijkheden te vermijden, wordt gepreciseerd dat dit artikel 122 dient te worden geïnterpreteerd onverminderd artikel 127/1. De bewaring en de andere soorten van verwerkingen waarvoor de operatoren gemachtigd zijn krachtens artikel 122 nemen immers niet weg dat de operatoren verplicht zijn tot inwilliging van de verzoeken om inzage vanwege de autoriteiten die in overeenstemming met artikel 127/1 van deze wet zijn geformuleerd.
Art. 5	Art. 5
L'article 123 renvoie dorénavant aux « données de localisation autres que les données relatives au trafic » pour mieux refléter l'intitulé de l'article 9 de la directive « vie privée et communications électroniques » (directive 2002/58/CE) qu'il transpose. La signalisation mobile contient certaines données de localisation sous la forme de « mises à jour de localisation ».	Artikel 123 verwijst voortaan naar "andere locatiegegevens dan verkeersgegevens" om het opschrift van artikel 9 van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) die het omzet, beter te weerspiegelen. In de mobiele signalisatie zitten bepaalde locatiegegevens in de vorm van "locatie-updates".
Les données de localisation qui constituent des données de trafic sont traitées par l'article 122 de la loi télécom.	Locatiegegevens die verkeersgegevens vormen, worden behandeld in artikel 122 van de telecomwet.

En outre, l'article 123 est complété pour tenir compte des évolutions techniques et légales.	Bovendien wordt artikel 123 aangevuld om rekening te houden met de technische en wettelijke ontwikkelingen.
L'alinéa 1er du paragraphe 1er confirme qu'un opérateur est autorisé à traiter des données de localisation pour répondre à une obligation légale.	Het eerste lid van paragraaf 1 bevestigt dat een operator locatiegegevens mag verwerken om aan een wettelijke verplichting te voldoen.
Ainsi, par exemple, un opérateur pourrait recevoir une injonction d'une autorité de geler certaines données de localisation (conservation rapide), comme prévu dans l'arrêt Quadrature du Net du 6/10/2020 de la CJUE (affaires C 511/18, C 512/18 et C 520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone).	Zo zou een operator van een autoriteit een bevel kunnen krijgen om bepaalde locatiegegevens te bevriezen (snelle bewaring), zoals bepaald in het arrest Quadrature du Net van 6/10/2020 van het HvJ-EU (de zaken C 511/18, C 512/18 en C 520/18: La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone).
Un autre exemple est la fourniture par un opérateur de données de localisation à une autorité (par exemple les autorités judiciaires, les services de renseignement et de sécurité ou la Cellule des personnes disparues de la Police Fédérale) pour répondre à sa demande. Cette autorité ne pourra bien entendu exiger de telles données que si cela est prévu dans sa législation organique.	Een ander voorbeeld is de verstrekking door een operator van locatiegegevens aan een autoriteit (bijv. de gerechtelijke autoriteiten, de inlichtingen- en veiligheidsdiensten of de cel Vermiste Personen van de federale politie) om aan haar verzoek te voldoen. Deze autoriteit zal zulke gegevens uiteraard maar mogen eisen als die is vastgelegd in haar organieke wet.
Le paragraphe 2 ne vise plus le retrait temporaire ou définitif du consentement, étant donné qu'une telle distinction n'est pas prévue dans la notion de consentement au sens du RGDP.	Paragraaf 2 beoogt niet langer de tijdelijke of definitieve intrekking van de toestemming aangezien het begrip van toestemming in de zin van de AVG niet voorziet in een dergelijk onderscheid.
Lorsque l'opérateur doit traiter des données pour les fournir à une autorité, c'est sa Cellule de coordination qui devra intervenir pour ce traitement.	Wanneer de operator gegevens moet verwerken om ze aan een autoriteit te verstrekken, zal zijn Coördinatiecel voor die verwerking moeten zorgen.
Afin d'écarter toute ambiguïté potentielle, il est précisé que le présent article 123 se comprend sans préjudice de l'article 127/1. En effet, la conservation et les autres types de traitements autorisés dans le chef des opérateurs sur le pied de l'article 123 n'excluent pas l'obligation pour les opérateurs de faire droit aux demandes d'accès des autorités formulées conformément à l'article 127/1 de la présente loi.	Om alle mogelijke onduidelijkheden te vermijden, wordt gepreciseerd dat dit artikel 123 dient te worden geïnterpreteerd onverminderd artikel 127/1. De bewaring en de andere soorten van verwerkingen waarvoor de operatoren gemachtigd zijn krachtens artikel 123 nemen immers niet weg dat de operatoren verplicht zijn tot inwilliging van de verzoeken om inzage vanwege de

	autoriteiten die in overeenstemming met artikel 127/1 van deze wet zijn geformuleerd.
Art. 6	Art. 6
Par son arrêt du 22 avril 2021 (n°57/2021), la Cour constitutionnelle a annulé l'abrogation de l'article 125, § 2, de la loi du 13 juin 2005. Il convient de réintroduire cette abrogation, qui permet de simplifier cette loi.	In zijn arrest van 22 april 2021 (nr. 57/2021) heeft het Grondwettelijk Hof de opheffing van artikel 125, § 2, van de wet van 13 juni 2005 vernietigd. Deze opheffing, die deze wet kan vereenvoudigen, dient opnieuw te worden ingevoerd.
Art. 7	Art. 7
Certaines modifications ont été apportées à l'article 126 de manière à s'aligner sur la terminologie et les définitions employées par le Code des communications électroniques européen dans la loi télécom (Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen).	Bepaalde wijzigingen werden aangebracht in artikel 126 om zich te conformeren aan de terminologie en definities gebruikt door het Europees wetboek voor elektronische communicatie in de telecomwet (Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie).
Premièrement, concernant le paragraphe 1er et vu que la notion de service de communications électroniques est définie dans le Code de manière plus large qu'actuellement, il n'est plus nécessaire de viser les opérateurs et les fournisseurs de services mais il suffit de viser les opérateurs.	Allereerst wat betreft paragraaf 1 en aangezien het begrip van elektronische-communicatiedienst in het Wetboek ruimer gedefinieerd is dan nu het geval is, is het niet meer noodzakelijk om de operatoren en de aanbieders van diensten te beogen, maar volstaat het om de operatoren te beogen.
Deuxièmement, le texte vise les services de communications interpersonnelles, pour reprendre la terminologie du Code, et non plus uniquement le service de téléphonie et le service de courrier électronique par internet.	Ten tweede, beoogt de tekst de interpersoonlijke communicatiediensten om de terminologie van het Wetboek over te nemen, en niet langer enkel de telefoniedienst en de dienst van e-mail via internet.
Il convient de rappeler que si un opérateur ne traite pas de données à conserver ni ne les génère, l'obligation de conserver des données est en pratique sans objet pour lui.	Er dient te worden aan herinnerd dat indien een operator de te bewaren gegevens niet verwerkt en niet genereert, de verplichting tot gegevensbewaring in de praktijk zonder voorwerp is voor hem.
Pour mettre en œuvre l'arrêt de la Cour constitutionnelle du 22 avril 2021 et l'arrêt	Voor de tenuitvoerlegging van het arrest van het Grondwettelijk Hof van 22 april 2021 en het

<p>Quadrature du Net de la Cour de Justice de l'Union européenne, ne sont plus visées par l'obligation de conservation que les données de souscription et les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique (tels que l'identifiant créé pour chaque communication). Le présent article est applicable lorsqu'un service de communications électroniques est fourni en Belgique.</p>	<p>arrest-Quadrature du Net van het Europees Hof van Justitie worden voor de bewaringsplicht enkel nog de abonnementsgegevens en technische gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst beoogd, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie (zoals de identificatiecode die wordt gecreëerd voor elke communicatie). Dit artikel is van toepassing wanneer elektronische-communicatiedienst in België wordt verstrekt.</p>
<p>La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave.</p>	<p>De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit.</p>
<p>Une distinction est effectuée entre l'adresse IP utilisée pour souscrire au service et les autres adresses IP. En effet, l'adresse IP utilisée pour souscrire au service est une donnée qui doit être conservée par l'opérateur dans le cadre de l'article 127, afin de pouvoir établir ou vérifier l'identité de l'abonné.</p>	<p>Er wordt een onderscheid gemaakt tussen het IP-adres dat gebruikt is om op de dienst in te tekenen en de overige IP-adressen. Het IP-adres dat gebruikt is om in te tekenen op de dienst is immers een gegeven dat door de operatoren moet worden bewaard in het kader van artikel 127, om de identiteit van de abonnee te kunnen vaststellen of nagaan.</p>
<p>Les données de souscription comprennent entre autres le numéro de téléphone, l'adresse email, le numéro d'abonné, la date de début et de fin de la souscription. Le Conseil d'Etat français, qui a été amené à examiner la législation française en matière de conservation de données de trafic pour les autorités (arrêt du 21/04/2021 nos 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), a considéré à cet égard ce qui suit : « il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement</p>	<p>De abonnementsgegevens omvatten onder andere het telefoonnummer, het e-mailadres, het nummer van de abonnee, de start- en einddatum van het abonnement. De Franse Conseil d'Etat, die de Franse wetgeving betreffende bewaring van verkeersgegevens voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), heeft daarover het volgende gesteld: "uit de richtlijn van 12 juli 2002 en van de AVG blijkt duidelijk dat zij niet gekant zijn tegen een verplichting tot algemene en ongedifferentieerde bewaring, voor de duur van een jaar, van andere inlichtingen dan die in verband met de burgerlijke identiteit die verstrekt zijn bij het sluiten van een contract door een gebruiker of bij het aanmaken van een account enerzijds, en van de gegevens met</p>

aux 3° et 4° de l'article 1er du décret du 25 février 2011 » (point 36).	betrekking tot de betalingen anderzijds, respectievelijk vermeld in de bepalingen onder 3° en 4° van artikel 1 van het decreet van 25 februari 2011" (punt 36) (vrij vertaald).
Les identifiants techniques qui ne sont pas rattachés à une communication déterminée mais qui servent principalement à identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé comprennent entre autres l'adresse IP source, l'IMEI (International Mobile Equipment Identity), l'IMSI (International Mobile Subscriber Identity), l'ICCID (Integrated Circuit Card Identifier), l'adresse MAC, le MSISDN (Mobile Station Integrated Services Digital Network), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées. A ce jour, la Cour de justice de l'Union européenne ne s'est prononcée que sur l'adresse IP source mais pas sur les autres données techniques précitées, dont la conservation est également nécessaire à des fins d'identification.	De technische identificatiecodes die niet gelinkt zijn aan een specifieke communicatie maar die hoofdzakelijk dienen om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, omvatten onder andere het IP-bronadres, de IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), ICCID (Integrated Circuit Card Identifier), het MAC-adres, het MSISDN (Mobile Station Integrated Services Digital Network), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën. Tot op heden heeft het Hof van Justitie van de Europese Unie zich enkel uitgesproken over het IP-adres aan de bron, maar niet over de voormelde andere technische gegevens, waarvan de bewaring eveneens noodzakelijk is voor identificatiedoeleinden.
Les données nécessaires pour identifier l'utilisateur final, l'équipement ou le service de communications électroniques peuvent inclure des données de trafic. A titre d'exemple, la conservation de certaines données de trafic sera nécessaire pour relier l'adresse IP à une personne spécifique ou pour retrouver le numéro de téléphone utilisé ou le numéro MSISDN (« Mobile Subscriber Integrated Services Digital Network », à savoir le numéro de téléphone avec le préfixe international) servi.	De gegevens die noodzakelijk zijn om de eindgebruiker, de apparatuur of de elektronische-communicatiedienst te identificeren, kunnen verkeersgegevens omvatten. Zo zullen bijvoorbeeld bepaalde verkeersgegevens moeten bewaard worden om het IP-adres aan een specifieke persoon te linken of om het gebruikte telefoonnummer of MSISDN-nummer ("Mobile Subscriber Integrated Services Digital Network", met name het telefoonnummer met het internationale prefix) terug te vinden.
Comme l'indique la CJUE dans son arrêt Quadrature du Net du 6/10/2020, l'adresse IP source est le seul moyen susceptible de permettre l'identification de l'auteur d'une infraction en ligne (point 154 de l'arrêt).	Zoals aangegeven in het arrest-Quadrature du Net van het HvJ-EU van 6/10/2020, is het IP-bronadres het enige middel aan de hand waarvan de dader van een online-inbreuk kan worden geïdentificeerd (punt 154 van het arrest).
Dans l'arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal (C-207/16, point 20), a été considérée comme ne constituant pas une ingérence grave aux droits fondamentaux (vie privée et protection des données à caractère personnel), la demande de la police judiciaire,	In het arrest van het HvJ-EU van 2 oktober 2018, Ministerio Fiscal (C207/16, punt 20), werd beschouwd dat het volgende geen ernstige inmenging vormt in de grondrechten (persoonlijke levenssfeer en bescherming van de persoonsgebonden gegevens): het

pour les besoins d'une enquête pénale, de se voir transmettre les numéros de téléphone activés, pendant une période de douze jours, avec le code relatif à l'identité internationale d'équipement mobile (ci-après le « code IMEI ») du téléphone mobile volé ainsi que les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code.	verzoek van de gerechtelijke politie, ten behoeve van een strafrechtelijk onderzoek, om de telefoonnummers te krijgen die gedurende een periode van twaalf dagen werden geactiveerd aan de hand van de code voor de internationale identiteit van het mobiele toestel (hierna de "IMEI-code") van de gestolen mobiele telefoon alsook de persoonsgebonden gegevens met betrekking tot de burgerlijke identiteit van de houders of van de gebruikers van de telefoonnummers die overeenstemmen met de via deze code geactiveerde simkaarten.
Au vu de l'utilité que représentent ces données techniques afin de permettre l'identification d'auteurs d'infractions en ligne ou hors ligne, la mesure de conservation prévue est proportionnée.	In het licht van het nut dat deze technische gegevens vertegenwoordigen voor de identificatie van daders van overtredingen online en offline, is de geplande bewaringsmaatregel evenredig.
Art. 8	Art. 8
L'ancien article 126/1 de la LCE a été déplacé vers l'article 127/3 de la même loi. L'article 6 donne donc un contenu tout à fait nouveau à l'article 126/1.	Het oude artikel 126/1 van de WEC wordt door huidig wetsontwerp verplaatst naar artikel 127/3 van dezelfde wet. Artikel 6 geeft aan artikel 126/1 dus een volledig nieuwe inhoud.
La Cour de justice européenne a statué dans l'arrêt "Quadrature du Net" du 6 octobre 2020 que le droit de l'Union européenne, en particulier l'article 15, paragraphe 1 de la directive 2002/58, doit être interprété comme s'opposant à des mesures législatives prévoyant la conservation préventive, générale et sans discrimination, de données relatives au trafic et de données de localisation. La Cour constitutionnelle a suivi ce raisonnement dans son arrêt du 22 avril 2018, et a annulé (partiellement) la loi du 29 mai 2016 sur la collecte et la conservation des données dans le secteur des communications électroniques.	Het Europese Hof van Justitie heeft in het arrest "Quadrature du Net" van 6 oktober 2020 bepaald dat het Unierecht, meer bepaald artikel 15, paragraaf 1 van de richtlijn 2002/58 in die zin geïnterpreteerd moet worden dat het zich verzet tegen de wetgevende maatregelen die voorzien in een preventieve algemene en ongedifferentieerde bewaring van verkeersgegevens en locatiegegevens. Het Grondwettelijk Hof heeft deze redenering gevolgd in het arrest van 22 april 2021, en heeft de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (gedeeltelijk) vernietigd.
Afin de compenser l'absence de conservation généralisée des données relatives au trafic et à la localisation, le projet de loi actuel prévoit un combinaison de	Om het gebrek aan algemene bewaring van verkeers- en locatiegegevens op te vangen voorziet huidig voorontwerp van wet in een combinatie van uiteenlopende maatregelen,

<p>différentes mesures qui, ensemble, devraient permettre aux autorités judiciaires et aux services de renseignement de remplir leurs missions. L'accès aux données de communication est indispensable pour les enquêtes criminelles et les enquêtes à des fins de renseignement, tout comme la possibilité de disposer de données dites « historiques », c'est-à-dire de pouvoir remonter un certain laps de temps dans le passé, en examinant des données conservées antérieurement à la demande des autorités.</p>	<p>die gezamenlijk zowel de gerechtelijke autoriteiten als de inlichtingendiensten in staat moeten stellen om hun opdrachten te vervullen. De toegang tot de communicatiegegevens is onontbeerlijk, voor strafonderzoeken en onderzoeken met het oog op inlichtingen, net als de mogelijkheid om te beschikken over de zogenaamde "historische" data, d.w.z. de mogelijkheid om een bepaalde periode in het verleden terug te gaan, door gegevens te bestuderen die eerder op verzoek van de autoriteiten zijn bewaard.</p>
<p>Il convient également de noter que la conservation peut être bénéfique à la fois pour la victime, pour ses propres données (par exemple, dans les cas de harcèlement, il est important de pouvoir remonter dans le passé des données de la victime afin d'identifier l'origine d'un appel, d'un courriel ou d'un SMS), et pour l'accusé (les données de localisation peuvent prouver que l'accusé ne se trouvait pas sur la scène du crime au moment où celui-ci a été commis).). Il peut aussi s'agir d'identifier des témoins ce qui peut jouer à charge comme à décharge. (Parl. Chambre, 54-1567/001, p. 10-11).</p>	<p>Er moet trouwens ook gewezen worden op het feit dat de bewaring zowel in het voordeel kan zijn van het slachtoffer, voor zijn eigen gegevens (bijvoorbeeld, in zaken met betrekking tot belaging is het van belang om in het verleden van de gegevens van het slachtoffer te kunnen teruggaan met het oog op het identificeren van de oorsprong van een oproep, een e-mail of een sms), als van de beschuldigde (de lokalisatiegegevens kunnen aantonen dat de beschuldigde niet op de plaats van het misdrijf was op het tijdstip waarop het werd gepleegd). Het kan ook van belang zijn om getuigen te identificeren, wat zowel à charge als à décharge kan meespelen (Parl. St., Kamer, 54-1567/001, p. 10-11).</p>
<p>Dans son arrêt du 6 octobre 2020, la Cour de justice européenne a elle-même suggéré un certain nombre de pistes qui pourraient pallier l'absence d'un maintien général et sans discrimination. L'une d'entre elles est ce qu'on appelle la "conservation ciblée", qui fait l'objet du présent article.</p>	<p>Het Europese Hof van Justitie reikte in het arrest van 6 oktober 2020 zelf een aantal pistes aan die het gebrek aan een algemene en ongedifferentieerde bewaring kunnen opvangen. Eén van die pistes betreft de zogenaamde "gerichte bewaring", en is het voorwerp van huidig artikel.</p>
<p>En effet, la Cour a déclaré, en résumé, au paragraphe 168 :</p>	<p>Het Hof stelde immers, in de samenvattende paragraaf 168, het volgende:</p>
<p><i>« En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non</i></p>	<p><i>"Artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van</i></p>

<i>discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable. ».</i>	<i>categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd.”.</i>
La Cour s'est penchée sur les paragraphes 146 et suivants. Afin de mieux comprendre le présent article, il est utile de reproduire ici ces paragraphes (arrêt "Quadrature du Net", §§ 146 à 151).	Het Hof ging in de eerdere paragrafen 146 en volgende. Om huidig artikel beter te begrijpen is het nuttig om deze paragrafen hier over te nemen (arrest “Quadrature du Net, §§ 146 tot 151).
<i>« 146. En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation. »</i>	<i>“146. Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, a fortiori, bescherming van de nationale veiligheid – gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd – de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.”</i>
<i>147. Ainsi, comme l'a déjà jugé la Cour, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 108).</i>	<i>147. Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 108).</i>
<i>148. S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être</i>	<i>148. De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand</i>

<p><i>fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111).</i></p>	<p><i>van de categorieën betrokken personen, aangezien artikel 15, lid 1, van richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111).</i></p>
<p><i>149. À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.</i></p>	<p><i>149. In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zijn die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.</i></p>
<p><i>150. La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.</i></p>	<p><i>150. Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.</i></p>

<p>151. Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation. »</p>	<p>151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.”</p>
<p>La piste d'une conservation ciblée, dans laquelle une distinction est faite sur la base de personnes ou de zones géographiques, a déjà été analysée précédemment dans le cadre de la rédaction de la loi du 29 mai 2016. L'exposé des motifs de la loi dit à cet égard ce qui suit (Parl, Chambre, 54-1567/001, p. 12) :</p>	<p>De piste van een gerichte bewaring, waarin een onderscheid gemaakt wordt op grond van personen of geografische zones werd al eerder geanalyseerd naar aanleiding van de redactie van de wet van 29 mei 2016. De memorie van toelichting bij de wet zegt daarover het volgende (Parl St., Kamer, 54-1567/001, p. 12):</p>
<p>« Quant à la référence à une “zone géographique” ou un “cercle de personnes”, une activation de l'article 126 LCE sur base de ce type de critère s'apparenterait à du profilage avec les risques de discrimination qui en découlent. »</p>	<p>“Met betrekking tot de verwijzing naar een “geografische zone” of een “kring van personen” zou een activering van artikel 126 WEC op grond van dit type criterium op profilering lijken, met de risico's van discriminatie die eruit voortvloeien.”</p>
<p>Un examen plus approfondi de l'arrêt de la Cour de justice du 6 octobre 2020, et plus précisément des paragraphes cités ci-dessus, a conduit le gouvernement à conclure que la préservation ciblée avec une distinction basée sur les zones géographiques est effectivement une option, pour autant que cette distinction soit fondée sur des éléments objectifs et non discriminatoires. Au § 150, la Cour indique : « Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages ».</p>	<p>Nader onderzoek van de uitspraak van het Hof van Justitie van 6 oktober 2020, en meer bepaald van de hierboven geciteerde paragrafen, bracht de regering tot de conclusie dat een gerichte bewaring met een onderscheid op basis van geografische zones wel degelijk een optie is, zolang dat onderscheid gebaseerd is op objectieve en niet-discriminerende elementen. In § 150 zegt het Hof daarover het volgende: “Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.”</p>
<p>Le nouvel article 126/1 reprend certaines notions incontestées de l'ancien article 126</p>	<p>Het nieuwe artikel 126/1 herneemt bepaalde onbetwiste begrippen van het oude artikel</p>

de la loi sur les communications électroniques, et est structuré comme suit :	126 van de wet betreffende de elektronische communicatie, en is opgebouwd als volgt:
- le paragraphe 1 ^{er} contient le principe de l'obligation de conservation et la durée de conservation par défaut (12 mois), ainsi que les finalités de la conservation,	- paragraaf 1 bevat het principe en de standaardduur van de bewaarplicht (12 maanden), alsook de doeleinden van de bewaring,
- le paragraphe 2 définit les données à conserver,	- paragraaf 2 bepaalt de gegevens die bewaard worden,
- le paragraphe 3 indique d'une part les zones géographiques, qui, sur la base de données de statistiques de criminalité doivent faire l'objet d'une conservation temporaire des données ou, les zones qui vu le niveau général de la menace doivent également faire l'objet d'une conservation temporaire des données, et, d'autre part, les zones géographiques, qui vu leur nature spécifique doivent faire l'objet d'une conservation de données pendant 12 mois,	- paragraaf 3 geeft aan dat er aan de ene kant geografische zones zijn die, op basis van criminaliteitsstatistieken of op basis van het algemene dreigingsniveau, het onderwerp uitmaken van een tijdelijke bewaarplicht. Aan de andere kant zijn er ook geografische zones die, door hun specifieke aard het onderwerp uitmaken van een bewaarplicht gedurende 12 maanden,
- le paragraphe 4 précise certains aspect du concept de zones géographiques auxquelles la conservation se rapporte,	- paragraaf 4 définit le concept van geografische zones waarop de bewaring betrekking heeft,
- enfin, le paragraphe 5 donne quelques délégations au Roi, dont la possibilité de déterminer des zones supplémentaires sur la base des critères énumérés dans la loi.	- paragraaf 5, tenslotte, geeft een aantal delegaties aan de Koning, o.a. de mogelijkheid om op basis van de in de wet opgesomde criteria, aanvullende zones te bepalen op basis van hun specifieke aard.
Lien avec la législation générale en matière de protection de la vie privée	Verband met de algemene wetgeving inzake de bescherming van de persoonlijke levenssfeer
Le premier alinéa du paragraphe 1 ^{er} de l'article commence par prévoir qu'il s'applique sans préjudice des dispositions de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et du RGPD. La loi du 30 juillet 2018 est la loi générale qui s'applique en tout état de cause en matière de protection des données à caractère personnel. Outre la loi du 30 juillet 2018, l'article fait également référence au Règlement général sur la protection des données, le règlement européen ayant un	Het eerste lid van paragraaf 1 van het artikel start met te bepalen dat het van toepassing is onverminderd de bepalingen van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de GDPR. De wet van 30 juli 2018 is de algemene wet die in elk geval van toepassing is inzake de bescherming van persoonsgegevens. Naast de wet van 30 juli 2018, verwijst het artikel ook naar de Algemene Verordening Gegevensbescherming, de Europese verordening met rechtstreekse werking die

effet direct qui uniformise les règles relatives au traitement des données à caractère personnel par les entreprises privées et les autorités publiques dans toute l'Union européenne.	de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
La présente loi particularise et complète les règles générales en matière de protection des données prévues par la loi du 30 juillet 2018 et le GDPR au regard des communications électroniques. Dans le même sens, ce nouvel article 126/1 s'applique dans les limites légalement prévues et conformément aux règles générales de protection des données.	Deze wet preciseert en vervolledigt de algemene regels inzake gegevensbescherming waarin de wet van 30 juli 2018 en de GDPR voorzien met betrekking tot elektronische communicatie. In dezelfde zin is dit nieuwe artikel 126/1 van toepassing binnen de grenzen waarin de wet voorziet en overeenkomstig de algemene regels inzake gegevensbescherming.
Dès lors, les fournisseurs et opérateurs sont explicitement tenus de respecter l'ensemble des dispositions de la loi du 30 juillet 2018, en ce qui concerne notamment la qualité des données (exactitude, mise à jour, conservation sous une forme permettant l'identification des personnes concernées, etc.), les obligations du responsable de traitement (confidentialité, mesures techniques et organisationnelles, soustraction, etc.), et les droits de la personne concernée. Cette dernière conserve bien entendu ses droits: elle devra être informée par les fournisseurs et les opérateurs de la conservation de ses données pendant la période fixée par la loi, elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier. Il va de soi que la personne concernée ne peut accéder qu'à ses données personnelles et pas aux données d'autres personnes.	Daarom zijn de operatoren uitdrukkelijk verplicht alle bepalingen van de wet van 30 juli 2018 na te leven, wat betreft meer bepaald de kwaliteit van de gegevens (nauwkeurigheid, bijwerking, bewaring op een manier die het mogelijk maakt de betrokken personen te identificeren, enz.), de verplichtingen van de persoon die verantwoordelijk is voor de verwerking (vertrouwelijkheid, technische en organisatorische maatregelen, uitbesteding, enz.), en de rechten van de betrokken persoon. Deze laatste behoudt uiteraard zijn rechten: de aanbieders en operatoren dienen de persoon op de hoogte te brengen van de bewaring van zijn gegevens gedurende de wettelijk vastgestelde periode; de persoon dient zijn gegevens te kunnen inzien en, indien nodig, deze te laten rechtzetten. Het spreekt vanzelf dat de betrokken persoon slechts zijn persoonlijke gegevens kan inkijken en niet de gegevens van andere personen.
Il est par ailleurs important de rappeler que dès lors que les données doivent être conservées à titre préventif par les opérateurs sur la base de cet article l'ensemble des services qui disposent d'une base légale et du besoin d'en connaître peuvent selon leur procédure ad hoc accéder à ces données.	Wij achten het ook nuttig erop te wijzen dat, aangezien de gegevens op basis van dit artikel door de operatoren voor preventieve doeleinden moeten worden bewaard, alle diensten met een rechtsgrondslag en een need-to-know toegang kunnen krijgen tot deze gegevens overeenkomstig hun ad hoc procedure.
Les entreprises tenues de conserver des données	De ondernemingen die verplicht zijn tot de bewaring van gegevens
L'alinéa 1 ^{er} du paragraphe 1 ^{er} traite également le champ d'application de l'article, qui s'applique à la fois aux opérateurs	Het eerste lid van paragraaf 1 behandelt ook het toepassingsgebied van het artikel, dat van toepassing is op zowel operatoren die

fournissant des services de communication, y compris de téléphonie, ou des services d'accès à Internet aux utilisateurs finals et aux opérateurs fournissant des réseaux de communications électroniques sous-jacents.	aan de eindgebruikers communicatiediensten, met inbegrip van telefonie, of internettoegangsdiensten aanbieden, als de operatoren die onderliggende elektronische communicatienetwerken aanbieden.
Le paragraphe 1 ^{er} précise en outre que les données ne sont conservées par les opérateurs concernés que dans la mesure où ces données ont été générées ou traitées par eux dans le cadre de la fourniture des services de communication concernés, et uniquement dans les zones géographiques prédéfinies. En d'autres termes, il n'y a aucune obligation de conserver les données lorsque celles-ci :	Paragraaf 1 preciseert verder dat de gegevens enkel bewaard worden door de betrokken operatoren voor zover deze gegevens werden gegenereerd of behandeld door hen in het kader van de verstrekking van de betrokken communicatiediensten, en enkel binnen de vooraf bepaalde geografische zones. Er is m.a.w. geen verplichting gegevens te bewaren wanneer deze:
1° ne sont pas générés ou traités par les opérateurs concernés,	1° niet gegenereerd of verwerkt worden door de betrokken operatoren,
2° ne sont pas générés ou traités dans les zones géographiques déterminées au paragraphe 3.	2° niet gegenereerd of verwerkt worden binnen de geografische zones bepaald in paragraaf 3.
Finalités de la conservation	Doeleinden van de bewaring
Le paragraphe 1er prévoit également que les 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.	Paragraaf 1 bepaalt ook dat de gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid de bescherming van de vitale belangen van een natuurlijke persoon.
A cet égard, nous pouvons noter que la finalité de la lutte contre les infractions graves, pour laquelle ces données sont conservées et peuvent être demandées, comprend également une enquête portant sur un éventuel abus de marché menée par l'auditeur de la FSMA. Les infractions à l'interdiction des abus de marché (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)) constituent en effet un délit grave (voir également le commentaire de l'article 30 du présent projet de loi). Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet considérable. Il s'agit au sein du secteur financier, de l'une des infractions les plus	In dit verband kan worden opgemerkt dat onder het doel van de strijd tegen zware criminaliteit waarvoor deze gegevens worden bewaard en kunnen worden opgevraagd, ook een onderzoek naar marktmisbruik door de auditeur van de FSMA valt. Inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), maken immers een ernstig misdrijf uit (zie ook de toelichting bij artikel 30 van onderhavig wetsontwerp). De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de meest ernstige inbreuken,

<p>graves, comme en témoignent également le fait que le règlement relatif aux abus de marché exige pour ces infractions des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières européennes, et le fait que la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché exige que les États membres prévoient également des sanctions pénales pour les abus de marché (élaborées dans les articles 39 et 40 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, qui prévoient des peines d'emprisonnement maximales de quatre ans, et de quatre et deux ans respectivement).</p>	<p>wat o.m. blijkt uit het feit dat de Verordening marktmisbruik voor deze inbreuken aanzienlijk hogere minimale maximumboetes vereist dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere Europese financiële wetgeving, alsook uit het feit dat Richtlijn 2014/57/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende strafrechtelijke sancties voor marktmisbruik de lidstaten oplegt om voor marktmisbruik ook strafrechtelijke sancties te voorzien (uitgewerkt in de artikelen 39 en 40 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, die voorzien in maximale gevangenisstraffen van vier jaar, respectievelijk vier en twee jaar).</p>
<p>Les données à conserver</p>	<p>De te bewaren gegevens</p>
<p>Le paragraphe 2 de l'article 126/1 énumère les données qui doivent être conservées par les opérateurs. Ce paragraphe ne contient aucun élément nouveau par rapport à l'ancien article 126, annulé par la Cour constitutionnelle. L'on peut se référer, à cet égard, à l'exposé des motifs de la loi du 29 mai 2016 (Doc. Parl., Chambre, 54-1567/001, p. 27).</p>	<p>In paragraaf 2 van het artikel 126/1 worden de gegevens opgesomd die door de operatoren bewaard zullen worden. Deze paragraaf bevat geen nieuwe elementen ten opzichte van het oude, door het Grondwettelijk Hof vernietigde artikel 126. Er kan verwezen worden naar de memorie van toelichting bij de wet van 29 mei 2016 (Parl. St., Kamer, 54-1567/001, p. 27)).</p>
<p>Pour ce qui concerne les données de communication visées au point 2°, il est rappelé explicitement que l'article ne couvre pas le contenu des communications. Par conséquent, la conservation du contenu de la communication n'est pas possible.</p>	<p>Voor wat betreft de communicatiegegevens bedoeld in punt 2° wordt overigens uitdrukkelijk herhaald dat het artikel geen betrekking heeft op de inhoud van communicaties. De bewaring van de inhoud van de communicatie is dus niet mogelijk.</p>
<p>L'alinéa 2 du deuxième paragraphe fait référence à un arrêté royal dans lequel sont déterminées les données à conserver par type de catégories et les exigences auxquelles ces données doivent correspondre. Cet arrêté royal existe déjà : il s'agit de l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques. Cet arrêté royal sera modifié pour couvrir aussi les données de la 5G. Il faut également le toiletter vu que l'arrêté royal du 19 septembre 2013 contient également des données d'identification qui sont maintenant visées par les articles 126</p>	<p>Het tweede lid van paragraaf 2 verwijst naar een koninklijk besluit waarin de te bewaren gegevens per type van categorie alsook de vereisten waaraan deze gegevens moeten beantwoorden bepaald worden. Dit koninklijk besluit bestaat al: het gaat om het Koninklijk Besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit koninklijk besluit zal aangepast worden om de 5G-gegevens te omvatten. Het moet ook bijgewerkt worden, aangezien het koninklijk besluit van 19 september 2013 ook identiteitsgegevens bevat die nu beoogd worden door de</p>

et 127 de la loi, et qui ne sont pas visées par le présent article 126/1.	artikelen 126 en 127 van de wet, en die niet voorzien zijn in het huidige artikel 126/1.
Les catégories de lieux où il peut y avoir une conservation de données : introduction	Categorieën van plaatsen waar gegevens kunnen worden opgeslagen: inleiding
Il est premièrement important de rappeler que l'identification dans la loi des catégories de lieux et des lieux où il peut y avoir une conservation des données implique, ipso facto, qu'il n'y a plus de conservation générale et indifférenciée de données de localisation ou de trafic puisque la détermination de ces lieux et de la durée de conservation des données y relative amènent un ciblage de la 'data retention' réalisée à titre préventif.	In de eerste plaats is het belangrijk eraan te herinneren dat de identificatie in de wet van de categorieën van plaatsen en van de plaatsen waar gegevens mogen worden bewaard, ipso facto impliceert dat er geen sprake meer is van een algemene en ongedifferentieerde bewaring van locatie- of verkeersgegevens, aangezien de vaststelling van deze plaatsen en van de duur van de bewaring van de daarop betrekking hebbende gegevens leidt tot een gerichte 'data retention' op preventieve basis.
Deuxièmement , le critère géographique suggéré par la Cour de Justice européenne est utilisé dans le présent article de deux façons complémentaires.	Ten tweede wordt het door het Europese Hof van Justitie voorgestelde geografische criterium in dit artikel op twee complementaire manieren gebruikt.
Il permet <u>d'une part</u> , de circonscrire les lieux caractérisés, comme le précise le point 150 de l'arrêt, par « un nombre élevé d'actes de criminalité grave » et <u>d'autre part</u> d'énumérer les lieux stratégiques, qui nécessitent en tant que tels de par leur nature (affectation, leur caractéristique, leur symbolique) une protection, notamment via l'instauration d'une conservation de données sur ces lieux car ils pourraient être la cible d'actes de criminalité grave ou être exposés à des menaces pour la sécurité nationale.	<u>Enerzijds</u> kunnen zo, zoals in punt 150 van het arrest wordt gesteld, plaatsen worden aangewezen die worden gekenmerkt door "een groot aantal daden van zware criminaliteit", en <u>anderzijds</u> kunnen strategische plaatsen worden aangewezen die wegens hun aard (gebruik, kenmerken of symboliek) bescherming behoeven, met name door de invoering van de bewaring van gegevens op deze plaatsen, omdat zij het doelwit kunnen zijn van zware criminaliteit of blootgesteld kunnen worden aan bedreigingen van de nationale veiligheid.
La détermination des zones géographiques	Bepaling van de geografische gebieden
En fonction des hypothèses visées dans le § 3 la zone géographiques sera définie par	Afhankelijk van de veronderstellingen in § 3 wordt het geografische gebied gedefinieerd door
- un ou plusieurs arrondissements (§3, alinéa 1 ^{er} , 1 ^o , 1 ^{er} tiret),	- een of meer arrondissementen (§ 3, 1 ^{ste} lid, 1 ^o , eerste streepje)
- une ou plusieurs zone de police (§ 3, alinéa 1 ^{er} , 1 ^o , second tiret),	- een of meer politiezones (§ 3, 1 ^{ste} lid, 1 ^o , tweede streepje)

- une ou plusieurs communes (par exemple dans le cadre des infrastructures critiques)	- een of meer gemeenten (bijvoorbeeld in het kader van de kritieke infrastructuur)
- une adresse ou plusieurs adresses (par ex: une ambassade ou un domaine provincial).	- een adres of verscheidene adressen (b.v. een ambassade of een provinciaal domein).
Comme le § 5 le précise, le Roi déterminera les paramètres techniques qu'un opérateur de réseau mobile (1), et un opérateur de réseau fixe (2) utilisent pour limiter la conservation de données aux zones visées au paragraphe 3.	Zoals vermeld in paragraaf 5, zal de Koning de technische parameters bepalen die een operator van een mobiel netwerk (1), en een operator van een vast netwerk (2) gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones.
Le § 4 précise aussi que les fournisseurs de services de communication sur Internet (les fournisseurs "over the top" tels que WhatsApp, Google, etc.) (3) peuvent utiliser les données les plus fiables et précises possible pour déterminer que l'utilisateur final de leur réseau ou service est situé dans une zone couverte par une obligation de conservation des données.	Paragraaf 4 bepaalt ook dat de aanbieders van communicatiediensten via internet (de "over the top" providers zoals WhatsApp, Google, etc) (3) de meest betrouwbare en nauwkeurige gegevens kunnen gebruiken om te bepalen dat de eindgebruiker van hun netwerk of dienst zich bevindt in een zone die gedekt is door een verplichting gegevens te bewaren.
Cette disposition n'a bien entendu pas pour but d'inciter les opérateurs à conserver davantage de données de localisation sur leurs utilisateurs. Cette disposition précise uniquement que les opérateurs utilisent les données qu'ils conservent ou traitent pour donner à leurs utilisateurs finaux l'accès à leur réseau ou service afin d'activer ou non la conservation des données pour cet utilisateur.	Het is niet de bedoeling dat operatoren door deze bepaling meer locatiegegevens gaan bijhouden over hun gebruikers. Deze bepaling maakt enkel duidelijk dat de operatoren de gegevens die ze bewaren of verwerken om hun eindgebruikers toegang te geven tot hun netwerk of dienst, kunnen toepassen om al dan niet de bewaring van gegevens voor die gebruiker aan te zetten.
Les réseaux mobiles savent en tout cas où se trouvent les utilisateurs finaux au niveau de l'antenne, car celle-ci est un élément nécessaire dans un réseau mobile. Chaque utilisateur final doit être localisé afin d'établir une connexion et de permettre la communication.	Mobiele netwerken weten sowieso waar de eindgebruikers zich bevinden op niveau van de antenne, omdat dit een noodzakelijk gegeven is in een mobiel netwerk. Elke eindgebruiker moet namelijk kunnen worden gelokaliseerd om een verbinding op te stellen en communicatie mogelijk te maken.
Les réseaux fixes utilisent une paire de cuivre, la distribution par câble ou un réseau en fibre optique pour fournir un accès au réseau ou des services à leurs utilisateurs finaux. La difficulté avec les utilisateurs fixes est que la relation entre le lieu d'utilisation du service et l'adresse de facturation ne correspond pas nécessairement (un employeur peut par exemple prendre à sa charge l'abonnement d'un employé). Afin d'éviter que les opérateurs n'aient à comparer en permanence les différentes	Vaste netwerken maken gebruik van een koper-, de kabel- of een glasvezelnetwerk om toegang tot het netwerk of diensten te kunnen aanbieden aan hun eindgebruikers. De moeilijkheid bij vaste gebruikers is dat de relatie tussen plaats van gebruik van de dienst en het facturatieadres niet per se overeenkomt. Om te vermijden dat verschillende gebruikersgegevens door de operatoren continu moeten worden vergeleken, zijn de aggregatiepunten opgenomen die de zone dekken. Een

<p>données des utilisateurs, des points d'agrégation ont été inclus pour couvrir la zone. Un point d'agrégation est le point de connexion d'où partent les paires de cuivre, la distribution par câble ou la fibre optique pour les utilisateurs individuels. Un point d'agrégation couvre généralement une ou plusieurs rues, ce qui en fait un paramètre idéal pour la détermination des zones.</p>	<p>aggregatiepunt is het aansluitingspunt van waaruit het koper-, kabel- of glasvezelnetwerk vertrekt naar de individuele gebruikers. Meestal dekt een aggregatiepunt een of meerdere straten, wat het een ideale parameter maakt om de zones te kunnen af te baken.</p>
<p>Pour les fournisseurs de services de communication fournis via Internet, cette disposition prévoit qu'ils peuvent utiliser les données de localisation de leurs utilisateurs finaux dont ils disposent pour déterminer s'ils doivent conserver les métadonnées sur ces utilisateurs. Les données de localisation dont disposent ces fournisseurs sont diverses, mais il s'agit souvent de données de localisation très précises, allant jusqu'à la précision des systèmes de positionnement par satellite. Les utilisateurs ont par ailleurs donné leur accord lorsqu'ils s'inscrivent au service, et ces données de localisation constituent un élément essentiel du modèle de revenus de ces fournisseurs, dont les applications sont très souvent commercialisées.</p>	<p>Voor de aanbieders van communicatiediensten die via internet worden geleverd voorziet deze bepaling dat zij gebruik kunnen maken van de lokalisatiegegevens die ze van hun eindgebruikers hebben om te bepalen of ze metadata over deze gebruikers moeten bijhouden. De lokalisatiegegevens die deze aanbieders hebben is divers, maar vaak gaat het om zeer precieze lokalisatiegegevens, tot de precisie van satellietplaatsbepalingssystemen toe. De gebruikers hebben hier bij het registreren van de dienst hun akkoord voor gegeven, en deze lokalisatiegegevens vormen een wezenlijk onderdeel van het verdienmodel van deze aanbieders, wiens applicaties zeer vaak gratis op de markt worden gezet.</p>
<p>Concrètement, si une personne bouge d'une zone où il y a de la conservation de données à une autre où il n'y en a pas, seules les données qui sont capturées dans la zone où il y a une conservation de données feront l'objet d'une conservation au titre du présent article.</p>	<p>In concreto, wanneer een persoon zich beweegt van een gebied waar gegevens worden bewaard naar een ander gebied waar geen gegevens worden bewaard, zullen alleen de gegevens die zijn geregistreerd in het gebied waar wel gegevens worden bewaard, onderworpen zijn aan de bewaring uit hoofde van dit artikel.</p>
<p>Autrement formulé, les métadonnées d'une communication passant d'un mât ou d'un point d'agrégation à l'intérieur de la zone où il y a une 'data retention' à un mât ou à un point d'agrégation à l'extérieur de la zone (où il n'y a pas de 'data retention') ne sont conservées que partiellement c'est-à-dire uniquement dans la zone soumise à la conservation des données.</p>	<p>Met andere woorden, de metagegevens van een communicatie die, van een mast of aggregatiepunt binnen een gebied waar gegevens worden bewaard, overgaan naar een mast of aggregatiepunt buiten het gebied (waar dus geen gegevens worden bewaard), worden slechts gedeeltelijk bewaard, d.w.z. alleen in het gebied dat onder de gegevensbewaring valt.</p>
<p>Par contre toutes les communications seront conservées dans les zones soumises à une conservation de données, par exemple tout appel mobile effectué depuis ou envoyé vers cette zone géographique.</p>	<p>Echter, in gebieden waarvoor dataretentie geldt zullen alle verkeersgegevens van de communicatie worden bewaard, bijvoorbeeld alle mobiele telefoongesprekken die vanuit of naar dat geografische gebied worden gevoerd.</p>

<p>Enfin, un opérateur fournissant un service nomade doit réaliser des efforts raisonnables pour localiser et stocker les données relatives au trafic des communications par le service. La localisation des services nomades peut être effectuée, par exemple, via la localisation IP ou le point de connexion Wi-Fi où la communication s'établit. De cette manière, il est possible de déterminer si la communication se poursuit ou non dans une zone couverte par la conservation des données.</p>	<p>Tenslotte moet een operator die een nomadische dienst aanbiedt, een redelijke inspanning doen om communicaties via deze dienst te kunnen lokaliseren en er verkeersgegevens van op te slaan. De lokalisatie van nomadische diensten kan bijvoorbeeld via IP-lokalisatie of het wifi-aansluitingspunt waar de communicatie uitbreekt, worden uitgevoerd. Zo kan er worden bepaald of de communicatie al dan niet in een door dataretentie gedekte zone doorgaat.</p>
<p>Si l'opérateur ne parvient pas à localiser le service nomade avec suffisamment de précision, il doit raisonnablement supposer que le service nomade se trouve dans une zone couverte par la conservation de données, afin d'éviter de violer le §1.</p>	<p>Slaagt de operator niet in om de nomadische dienst afdoende precies te lokaliseren, dan moet die redelijkerwijs er van uitgaan dat de nomadische dienst valt in een door de dataretentie gedekte zone, om te vermijden dat de operator §1 zou schenden.</p>
<p>Le premier critère géographique : la conservation sur la base de lieux caractérisés par un nombre élevé d'actes de criminalités graves</p>	<p>Het eerste geografische criterium: retentie op basis van plaatsen die worden gekenmerkt door een hoog aantal daden van zware criminaliteit</p>
<p>Comme nous l'avons déjà énoncé, les données de la 'data retention' sont très importantes au niveau de la réalisation de la politique criminelle. En effet, les données de data retention permettent notamment d'établir dans le cadre des crimes violents (meurtres, viols, enlèvements, carjacking), qui est actif dans la région autour des scènes de crimes, de pouvoir localiser le téléphone portable utilisé et le moment de son utilisation, ou encore d'identifier un téléphone portable utilisé au moment des faits (en utilisant par exemple la localisation basée sur les antennes). A l'identique, dans le cadre de recherches liées à un réseau d'auteurs, il est nécessaire pour les enquêteurs, de déterminer sur la base des données de 'data retention', qui a été en contact avec qui et où se trouvent les lieux de rencontre possibles.</p>	<p>Zoals reeds aangehaald, zijn gegevens over 'data retentie' van groot belang voor de uitvoering van het criminaliteitsbeleid. In het geval van geweldsmisdrijven (moorden, verkrachtingen, ontvoeringen, carjackings) kunnen gegevens van data retentie worden gebruikt om na te gaan wie actief is in de omgeving van de plaats van het misdrijf, om de gebruikte mobiele telefoon te lokaliseren en wanneer deze is gebruikt, of om nog een mobiele telefoon te identificeren die in gebruik was op het tijdstip van het misdrijf (bv. door gebruik te maken van locatiebepaling op basis van de antennes). Evenzo moeten de onderzoekers bij het onderzoek naar een dadernetwerk op basis van gegevens van 'data retentie' bepalen wie met wie contact heeft gehad en waar de mogelijke ontmoetingsplaatsen zijn.</p>
<p>Il est dès lors tout à fait logique qu'un critère lié à la commission d'actes de criminalité soit retenu dans le présent projet. Il serait par contre non fondé et totalement arbitraire de choisir a priori de n'imposer la conservation</p>	<p>Het is dan ook niet meer dan logisch dat een criterium dat verband houdt met het plegen van criminele feiten in dit ontwerp wordt weerhouden. Anderzijds zou het ongegrond en volstrekt willekeurig zijn om a priori te</p>

<p>que de certaines des données énumérés au § 2. En effet, comme les exemples énumérés ci-dessus le montrent tant les données de localisation que celles du trafic sont nécessaires à la réalisation des enquêtes. Il va cependant de soi que, dans le cadre des requêtes faites aux opérateurs, le magistrat peut bien entendu cibler sa demande.</p>	<p>kiezen voor het bewaren van slechts een deel van de gegevens die zijn opgesomd in § 2. Zoals uit de hierboven genoemde voorbeelden blijkt, zijn immers zowel locatiegegevens als verkeersgegevens noodzakelijk voor onderzoeken. Het spreekt voor zich dat de rechter, in het kader van verzoeken aan operatoren, zijn verzoek uiteraard kan toespitsen.</p>
<p>Au niveau du seuil de criminalité retenu pour élaborer des statistiques de criminalité, et donc pour déterminer un seuil en matière de 'data retention', le présent article tient compte des infractions graves énumérées à l'article 90ter du Code d'instruction criminelle. Le nombre de ces infractions par rapport au nombre d'habitants d'un arrondissement permet donc de déterminer s'il y aura ou pas une conservation ciblée de données au niveau arrondissemental. Les accès par la police à ces données sur la base de ce critère, se fera, sauf en cas de disparition inquiétante, toujours pour des infractions punies au moins par un an d'emprisonnement et sur la base des modalités prévues à l'article 90quater du Code d'instruction criminelle (autorisation d'un juge d'instruction qui détermine l'étendue des accès).</p>	<p>Wat betreft de misdaaddrempel die wordt gehanteerd voor het opstellen van misdaadstatistieken, en dus voor het bepalen van een drempel voor 'dataretentie', houdt dit artikel rekening met de ernstige inbreuken die zijn opgesomd in artikel 90ter van het Wetboek van Strafvordering. Het aantal van deze inbreuken in verhouding tot het aantal inwoners van een arrondissement zal dus bepalen of er al dan niet gerichte gegevensbewaring op arrondissementsniveau zal plaatsvinden. De toegang van de politie tot deze gegevens op basis van dit criterium zal, behalve in het geval van onrustwekkende verdwijningen, steeds geschieden voor inbreuken waarop een gevangenisstraf van ten minste één jaar staat en op basis van de modaliteiten van artikel 90quater van het Wetboek van Strafvordering (machtiging van een onderzoeksrechter die de omvang van de toegang bepaalt).</p>
<p>L'article 90ter reprend notamment des infractions :</p>	<p>Artikel 90ter omvat namelijk strafbare feiten:</p>
<p>- qui sont liées à la criminalité grave contre les personnes : par ex : attentat à la pudeur sur mineur et majeur et viol, enlèvement et recel de mineur, harcèlement par communications électroniques, ou</p>	<p>- die verband houden met zware criminaliteit tegen personen: bv. aanranding van minderjarigen en volwassenen en verkrachting, ontvoering en verbergings van minderjarigen, belaging via elektronische communicatie, of</p>
<p>- qui sont liées à la criminalité organisée (par ex organisation criminelle, traite des êtres humains, incitation à la débauche, l'embauche en vue de la débauche, le proxénétisme et la tenue de maison de débauche ainsi que l'offre et la vente (et non la simple détention) de matériel pédopornographique),</p>	<p>- die verband houden met de georganiseerde criminaliteit (bijvoorbeeld criminele organisatie, mensenhandel, aanzetten tot ontucht, tewerkstelling met het oog op ontucht, pooierschap en het houden van een bordeel, en de aanbidding en verkoop (niet louter het bezit) van kinderpornografie),</p>

<p>- ou encore d'autres infractions particulièrement graves qui permettent de mettre en branle des méthodes spécifiques de recueil d'information (par exemple, infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes, vols et extorsion de matière nucléaire et protection physique des matières nucléaires).</p>	<p>- of andere bijzonder ernstige inbreuken die specifieke methoden voor het vergaren van informatie in beweging zetten (bijvoorbeeld inbreuken tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en de door die systemen opgeslagen, verwerkte of doorgegeven gegevens, diefstal en afpersing van nucleair materiaal en fysieke beveiliging van nucleair materiaal).</p>
<p>L'arrêt du 6 octobre 2020 mentionne à propos de ce critère qu'il est « caractérisé par un nombre élevé d'actes de criminalité grave ». Il s'agit en d'autres termes de se baser sur des statistiques récentes qui peuvent démontrer ce nombre élevé d'actes de criminalité grave lequel va, à son tour, déterminer le risque élevé de commission d'infraction.</p>	<p>In het arrest van 6 oktober 2020 staat dat dit criterium "wordt gekenmerkt door een groot aantal daden van zware criminaliteit". Het gaat er met andere woorden om recente statistieken te gebruiken die dit grote aantal daden van zware criminaliteit kunnen aantonen, die op hun beurt het verhoogd risico op het plegen van strafbare feiten aantonen.</p>
<p>Le gouvernement a décidé de ne pas prendre un chiffre absolu qui serait identique pour tous ces lieux. Afin de tenir compte du principe de proportionnalité, il est en effet préférable d'opérer pour chaque lieux une pondération propre à sa situation criminogène. Ce seuil de criminalité grave, calculé par 1000 habitants permet donc de tenir compte de la réalité objective des phénomènes criminels au sein de chaque arrondissement, tout en permettant d'assurer une égalité de traitement pour l'ensemble de la population. En d'autres termes, ce critère permet de rencontrer le prescrit de la Cour de Justice et de la Cour constitutionnelle qui demande de mettre en œuvre des critères objectifs et non discriminatoires.</p>	<p>De regering heeft besloten geen absoluut cijfer te nemen dat voor al deze plaatsen identiek zou zijn. Teneinde rekening te houden met het evenredigheidsbeginsel verdient het de voorkeur elke plaats te wegen naar gelang van de criminogene situatie ervan. Deze drempel voor zware criminaliteit, berekend per 1.000 inwoners, maakt het dus mogelijk rekening te houden met de objectieve realiteit van de criminele fenomenen binnen elk arrondissement, en tegelijkertijd de gelijke behandeling van de gehele bevolking te waarborgen. Met andere woorden, dit criterium maakt het mogelijk te voldoen aan de eisen van het Hof van Justitie en het Grondwettelijk Hof, die de toepassing van objectieve en niet-discriminerende criteria vereisen.</p>
<p>Concrètement, le seuil annuel est de 3 faits graves (90 ter) par 1000 habitants sur une moyenne de 3 ans. Cette moyenne permet de lisser les pics et les chutes de criminalités, qui seraient dus à des épiphénomènes et permet donc d'objectiver ce seuil.</p>	<p>Concreet is gekozen voor een jaarlijkse drempel van gemiddeld 3 ernstige strafbare feiten (90 ter) per 1000 inwoners over een periode van 3 jaar. Het hanteren van een gemiddelde nivelleert pieken en dalen in de criminaliteit die aan tijdelijke fenomenen te wijten zouden zijn en laat dus toe om de drempel te objectiveren.</p>

Ce seuil, calculé par 1000 habitants permet d'une part de tenir compte de la réalité divergente des phénomènes criminels au sein des différents arrondissements

Illustrons ce propos :

- Pour l'arrondissement le plus peuplé, soit l'arrondissement d'Anvers (1 869 730 habitants en 2019), ce seuil revient à dire qu'il faut qu'il y ait eu en moyenne sur les 3 dernières années **5 609 faits graves**. Autrement formulé, sur les 3 dernières années, 16 827 faits graves se sont déroulés à Anvers.
- Pour l'arrondissement de Bruxelles, (1 218 255 habitants en 2019), ce seuil revient à dire qu'il faut, qu'il y ait eu, en moyenne sur les 3 dernières années **3 655 faits graves**. En d'autres termes, sur les 3 dernières années, 1 965 faits graves se sont déroulés à Bruxelles.
- Pour l'arrondissement le moins peuplé, comme Eupen (77 949 habitants en 2019), ce seuil implique qu'il y ait eu, en moyenne sur les 3 dernières années **234 faits graves**, soit, sur un total de 3 ans, **702 faits graves, ou sur un total de 3 ans, 2109 faits graves**.
- Pour un arrondissement comme Charleroi (583 928 habitants en 2019) ou Mons (762 912 habitants en 2019) ceci implique qu'il y ait eu respectivement **1 752** et **2 889** faits en moyenne sur les 3 dernières années ou sur un total de **3 ans, 5256 et 8667 faits graves**.
- Pour la Flandre occidentale (1 200 945 habitants en 2019), cela veut dire qu'il y ait eu, en moyenne sur les 3 dernières années **3 603 faits graves**, ou sur les 3 dernières années, **10 808 faits graves**.
- Pour la Flandre orientale (1 525 255 habitants en 2019), cela veut dire qu'il y ait eu, en moyenne sur les 3 dernières années **4 576 faits graves** ou sur les 3 ans dernières années, **13 728 faits graves**.

Deze drempel, berekend per 1000 inwoners laat toe om enerzijds rekening te houden met de werkelijkheid van uiteenlopende criminele fenomenen in de verschillende arrondissementen.

Bijvoorbeeld:

- In het dichtstbevolkte arrondissement Antwerpen (1.869.730 inwoners in 2019) houdt deze drempel in dat er in de afgelopen 3 jaar gemiddeld **5.609 zware feiten** moeten zijn geweest. Met andere woorden, de voorbije 3 jaar vonden er in Antwerpen 16.827 zware feiten plaats.
- In het gerechtelijk arrondissement Brussel (1.218.255 inwoners in 2019), betekent deze drempel dat er in de afgelopen drie jaar gemiddeld **3 655 zware feiten** moeten zijn geweest. Met andere woorden, de afgelopen 3 jaar hebben er in Brussel 1.965 ernstige incidenten plaatsgevonden.
- Voor het kleinste arrondissement (Eupen, 77.949 inwoners in 2019) betekent de drempel dat er de voorbije 3 jaar gemiddeld **234 zware feiten**, vastgesteld moeten zijn, of, op een totaal van 3 jaar, **702 zware feiten, of op een totaal van 3 jaar, 2109 zware feiten**.
- Voor Charleroi (583.928 inwoners in 2019) of Bergen (762.912 inwoners in 2019) ligt de drempel op respectievelijk gemiddeld **1.752** en **2.889 zware feiten** gedurende de laatste 3 jaren of op een totaal van **3 jaar op 5256 en 8667 zware feiten**.
- In West-Vlaanderen (1.200.945 inwoners in 2019) betekent dit dat er de voorbije 3 jaar gemiddeld **3.603 zware feiten**, of gedurende de laatste 3 jaar **10 808 zware feiten**, zouden moeten vastgesteld zijn.
- Voor Oost-Vlaanderen (1.525.255 inwoners in 2019) komt de drempel gedurende de 3 voorbije jaren neer op gemiddeld **4575 zware feiten** of gedurende de laatste drie jaar op **13 728 ernstige feiten**.

<p>En outre, dans l'optique de tenir compte du principe de proportionnalité, la période de conservation des données est également modulée sur la base du taux de criminalité grave : avec un seuil maximal de 12 mois.</p>	<p>Bovendien, rekening houdend met het evenredigheidsbeginsel, wordt de termijn van de bewaarplicht veranderd in functie van het aantal zware strafbare feiten, tot een maximum van 12 maanden.</p>
<p>Au plus il y a une activité criminelle grave (90 ter code d'instruction criminelle), au plus il y a, au sein de l'arrondissement, un enracinement des activités de criminalité organisée/grave et au plus, il est dès lors nécessaire de pouvoir investiguer le passé des communication, notamment pour établir les liens entre les différents groupes d'auteurs, dans le but de les démanteler ou, à tout le moins, de déstabiliser la criminalité organisée/grave.</p>	<p>Hoe meer zware criminaliteit (volgens artikel 90ter van het Wetboek van Strafvordering) hoe dieper de georganiseerde/criminele activiteiten in het district geworteld zijn, en dus hoe noodzakelijker het is om in de tijd terug te gaan, met name om verbanden te leggen tussen de verschillende dadergroepen, teneinde deze te ontmantelen of op zijn minst de georganiseerde/criminele activiteit te destabiliseren.</p>
<p>De la sorte,</p>	<p>Dit betekent:</p>
<p>-Pour les arrondissements judiciaires où il y a sur une moyenne de 3 ans, à partir de [3 et jusque 4] infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants, le délai de conservation est de 6 mois.</p>	<p>- Voor gerechtelijke arrondissementen waar er op basis van een gemiddelde van 3 jaar, vanaf [3 en tot 4] inbreuken sprake is zoals bedoeld in artikel 90 ter van het Wetboek van Strafvordering, per 1000 inwoners per jaar gedurende 3 jaar, bedraagt de bewaartermijn 6 maanden.</p>
<p>- Pour les arrondissements judiciaires où il y a sur une moyenne de 3 ans à partir de [5 et jusque 6] infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants, le délai de conservation est de 9 mois.</p>	<p>- Voor gerechtelijke arrondissementen waar er op basis van een gemiddelde van 3 jaar, vanaf [5 en tot 6] inbreuken sprake is zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering, per 1000 inwoners per jaar gedurende 3 jaar, bedraagt de bewaartermijn 9 maanden.</p>
<p>- Pour les arrondissements où il y a une moyenne égale ou supérieure à [7] infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an au cours des 3 dernières années, le délai de conservation est de 12 mois.</p>	<p>- Voor gerechtelijke arrondissementen waar sprake is van een gemiddelde gelijk aan of meer dan [7] inbreuken zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering, per 1000 inwoners per jaar gedurende 3 jaar, bedraagt de bewaartermijn 12 maanden.</p>
<p>Au niveau de l'étendue géographique retenue, le niveau arrondissemental est le plus approprié pour tenir compte de la criminalité grave visée à l'article 90 ter du Code d'instruction criminelle, vu que ce niveau correspond à la compétence d'un parquet du Procureur du Roi et donc à la réalisation d'une politique de répression.</p>	<p>Op het niveau van de geografische reikwijdte die wordt gehanteerd, is het arrondissementsniveau het meest geschikt om rekening te houden met de zware criminaliteit zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering, aangezien dit niveau overeenkomt met de bevoegdheid van een parket van een Procureur des</p>

	Konings en dus met de uitvoering van een rechtshandavingsbeleid.
La structure de la police judiciaire fédérale suit cette même organisation arrondissementale: il y a une direction Judiciaire d'enquête - appelée PJF - par arrondissement judiciaire.	De structuur van de federale gerechtelijke politie volgt dezelfde arrondissementale organisatie: er is één Federale gerechtelijke Politie - FGP genoemd - per gerechtelijk arrondissement.
Or, c'est cette même PJF qui est chargée des enquêtes concernant les plus graves commis sur son arrondissement judiciaire ; ce sont ces faits qui sont repris dans l'article 90ter CIC .	Deze zelfde FGP is verantwoordelijk voor onderzoeken naar de ernstigste misdrijven die in zijn gerechtelijk arrondissement zijn gepleegd; dit zijn de feiten die zijn opgenomen in artikel 90ter wetboek van strafvordering.
L'arrondissement judiciaire constitue également un tout cohérent par rapport à la population et à certains phénomènes de criminalité.	Het gerechtelijk arrondissement vormt ook een samenhangend geheel met betrekking tot de bevolking en bepaalde criminaliteitsfenomenen.
A cet égard, il faut aussi noter que les groupes d'auteurs sont, par ailleurs, très mobiles et se déplacent et que le crime organisé est par essence polycriminel. Se limiter d'office à certains lieux très ciblés au niveau local pour ce type de criminalité n'est pas approprié.	In dit verband moet ook worden opgemerkt dat dadergroepen bovendien zeer mobiel zijn en zich verplaatsen, en dat de georganiseerde criminaliteit in essentie polycrimineel is. Het lijkt niet juist om zich voor dit soort criminaliteit te beperken tot bepaalde zeer gerichte plaatsen op lokaal niveau.
Dans cette optique, l'approche des « territoires criminels » doit être prise en compte. Le criminologue canadien Maurice Cusson a montré dans ses études qu'on peut considérer trois types de territoires criminels : les sanctuaires, les terrains de chasse et les lieux de plaisir. En matière de crime organisé, ces territoires criminels sont d'une importance capitale pour mener l'action publique et l'action policière.	In dat opzicht is het relevant de beschrijving van de "criminele gebieden" in gedachten te houden. De Canadese criminoloog Maurice Cusson heeft in zijn studies aangetoond dat er drie soorten criminele gebieden zijn: toevluchtsoorden, jachtgebieden en plaatsen van plezier. Wat de georganiseerde misdaad betreft, zijn deze criminele gebieden van het grootste belang voor het optreden van de overheid en de politie.
<u>Les sanctuaires</u> sont les lieux où les criminels et leurs structures sont implantés. S'il est clair que les organisations criminelles sont généralement implantées dans les agglomérations, ce n'est pas une généralité et par exemple les bandes criminelles de motards ont souvent tendance à implanter leurs Clubhouse (chapter) dans des zones reculées ou plus rurales (zone industrielle, cafés de village ou habitation isolée) mais sont susceptibles de se déplacer en fonction	<u>Toevluchtsoorden</u> zijn de plaatsen waar criminelen en hun structuren zijn gevestigd. Hoewel het duidelijk is dat criminele organisaties over het algemeen in stedelijke gebieden gevestigd zijn, is dit geen algemene regel en bijvoorbeeld motorbendes hebben vaak de neiging hun clubhuizen (chapter) in afgelegen of meer landelijke gebieden te vestigen (industriegebieden, dorpscafés of afgelegen woningen), maar zullen vermoedelijk verhuizen in functie van de

de la réaction policière/judiciaire et de la concurrence entre certaines organisations.	politonele/gerechtelijke reacties en de concurrentie tussen bepaalde organisaties
<u>Les terrains de chasse</u> sont les lieux où les groupes d'auteurs et les organisations criminelles commettent leurs faits. Il s'agit traditionnellement des informations qui ressortent des rapports statistiques annuels montrant la localisation temps-espace des phénomènes criminels.	<u>Jachtgebieden</u> zijn de plaatsen waar dadergroepen en criminele organisaties hun feiten plegen. Dit is wat meestal naar voren komt uit de jaarlijkse statistische verslagen waarin de criminele fenomenen worden bestudeerd.
Les activités des organisations criminelles et des groupes d'auteurs ne peuvent pas être limitées géographiquement au territoire d'une ou plusieurs communes. En effet, se priver de données de communications dans certaines zones serait une erreur fondamentale. Cela nous obligerait à prendre des mesures encore plus intrusives pour pouvoir suivre leurs agissements, leurs méfaits et démontrer pénalement les éléments constitutifs d'une organisation (Article 324bis C.Pén. notamment).	De activiteiten van criminele organisaties en dadergroepen mogen geografisch niet beperkt blijven tot het grondgebied van één of meer gemeenten. Het zou zodus een fundamentele vergissing zijn om communicatiegegevens in bepaalde gebieden te ontzeggen. Dit zou ertoe leiden dat er meer intrusieve maatregelen gebruikt zouden worden om hun daden en hun wandaden te kunnen volgen en de constitutieve elementen van een organisatie strafrechtelijk te kunnen aantonen (met name artikel 324bis Strafwetboek).
<u>Les lieux de plaisirs</u> , ainsi nommés par Cusson, sont les endroits où le milieu criminel se retrouve et s'organise, où il « dépense » en partie ses gains criminels. Il s'agit d'établissements de l'Horeca, de salles de jeux clandestines, de bars à champagne ou d'établissements de prostitution. Beaucoup sont implantés dans les grandes villes et les agglomérations mais il est connu qu'un certain nombre se situent hors de celles-ci, le long de grandes nationales en pleine campagnes (RN 3 entre Liège et Leuven, RN 5 entre Couvin et Charleroi, route rurales en région frontalière du Tournaisis, ...). L'ensemble de ces lieux sont donc susceptibles d'être mêlés d'une manière directe (ex terrains de chasse) ou d'une manière plus lointaine (ex lieux de plaisir) à la commission d'infractions graves.	<u>De plaatsen van plezier</u> , zoals Cusson ze noemt, zijn de plaatsen waar het criminele milieu bijeenkomt en zich organiseert, waar zij een deel van haar criminele inkomsten "uitgeeft". Het zijn horecagelegenheden, clandestiene speelzalen, champagnebars en prostitutie-inrichtingen. Een aantal daarvan zijn gelegen in de grote steden en gemeenten, maar het is bekend dat vele zich buiten deze steden en gemeenten bevinden, langs de hoofdwegen op het platteland (RN 3 tussen Luik en Leuven, RN 5 tussen Couvin en Charleroi, plattelandswegen in de grensstreek van Tournaisis, enz.). Al deze plaatsen zijn dus vermoedelijk op directe (het voorbeeld van de jachtgebieden) of indirecte (voorbeeld van de plaatsen van plezier) manier verbonden met het plegen van zware misdrijven.
Enfin, si ce seuil n'est pas atteint au niveau d'un arrondissement et que donc, il n'y a pas de raison objective de réaliser une conservation préventive des données de trafic et de localisation au sein de cet arrondissement , alors la conservation des données de trafic et de localisation se fait uniquement à plus petite échelle et au niveau de la/les zones de police dans laquelle/lesquelles, par 1000	Ten slotte, indien deze drempel niet wordt bereikt op het niveau van een arrondissement en er dus geen objectieve reden is om in dit arrondissement een preventieve bewaring van verkeers- en locatiegegevens op te leggen , worden de verkeers- en locatiegegevens alleen bewaard op kleinere schaal, zijnde het niveau van de politiezone, waar minstens 3

<p>habitants par an au cours des 3 dernières années au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle ont été répertoriées</p> <p>A l'image de ce qui se passe au niveau arrondissemental, le délai de conservation est de 6 mois lorsque le taux d'infraction par 1000 habitants se situe entre 3 et 4 faits 90 ter du code d'instruction criminelle, de 9 mois, lorsque ce taux se situe entre 5 et 6 et de 12 mois lorsque ce taux est égal ou supérieur à 7 infractions 90 ter du Code d'instruction criminelle par 1000 habitants au cours des 3 dernières années.</p>	<p>strafbare feiten, zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering, per 1000 inwoners per jaar gedurende de voorbije 3 jaar zijn vastgesteld.</p> <p>De bewaartermijn bedraagt, naar analogie met de regeling op vlak van de arrondissementen, 6 maanden wanneer het aantal per 1000 inwoners per jaar 3 of 4 is, 9 maanden wanneer het aantal 5 of 6 is, en 12 maanden wanneer het aantal hoger dan 7 zware criminele feiten bedraagt, zoals bedoeld in art 90ter van het Wetboek van Strafvordering.</p>
Procédure pour les statistiques	Procedure voor statistieken
<p>La production annuelle de statistiques implique que ce critère est dynamique puisqu'il dépend des chiffres de criminalité repris soit au niveau d'un arrondissement, soit au niveau d'une zone de police.</p> <p>La période de référence d'un an permet d'avoir des statistiques suffisamment significatives tout en fournissant une image actuelle des chiffres de criminalité.</p>	<p>Het jaarlijks bepalen van statistieken impliceert dat dit criterium dynamisch is, aangezien het afhangt van de criminaliteitscijfers die hetzij op het niveau van een arrondissement, hetzij op het niveau van een politiezone worden geregistreerd.</p> <p>De referentieperiode van één jaar maakt het mogelijk voldoende betekenisvolle statistieken op te stellen en tegelijkertijd een actueel beeld van de criminaliteitscijfers te geven.</p>
L'arrêt du 6 novembre 2020 mentionne comme critère une « situation caractérisée par (...) un risque élevé de commission d'actes de criminalité grave ».	Het arrest van 6 november 2020 vermeldt als criterium een "situatie die wordt gekenmerkt door (...) een hoog risico op het plegen van zware criminele feiten".
Il s'agit donc de prendre comme point de référence la commission de telles infractions.	Het plegen van dergelijke strafbare feiten moet dus als referentiepunt genomen worden.
A cet égard, notons que les constatations d'infractions sont répertoriées au niveau national dans la Banque de données Nationale Générale, visée à l'article 44/7 de la loi sur la fonction de police.	De vaststellingen van strafbare feiten worden op nationaal niveau geregistreerd in de Nationale Algemene Gegevensbank, waarnaar in artikel 44/7 van de Politiewet wordt verwezen.
Le point 6 de cet article mentionne en effet que cette banque de données sert à aider à « l'appui à la définition et à la réalisation de la politique policière et de sécurité ».	In punt 6 van dit artikel wordt ook vermeld dat deze gegevensbank "het mogelijk maakt "de bepaling en de uitwerking van het politie- en veiligheidsbeleid te ondersteunen ".
Il faut bien être conscient que l'ensemble des faits criminels ne sont pas connus de la police (absence de plainte, non visibilité directe du phénomène, par exemple la	Er moet op gewezen worden dat er een groot aantal feiten is die niet door de politie vastgesteld worden (geen klacht ingediend, onzichtbaarheid van het fenomeen,

traite ou le trafic d'êtres humains). Dès lors, les faits répertoriés dans la B.N.G. ne constituent qu'une partie limitée des phénomènes criminels au niveau des arrondissements et des zones de police.	bijvoorbeeld mensenhandel/mensensmokkel). Hierdoor bevat de Algemene Nationale Gegevensbank slechts een beperkt deel van de criminele fenomenen die terug te brengen zijn tot het niveau van een gerechtelijk arrondissement en politiezone.
Concrètement, la direction de l'information et de l'ICT de la police fédérale réalisera une fois par an, les statistiques au niveau des arrondissements et le cas échéant, à l'intérieur de ces arrondissements au niveau des rues.	Concreet zal de Directie Informatie en ICT van de federale politie één keer per jaar statistieken opmaken op het niveau van de arrondissementen en, indien nodig, binnen deze arrondissementen op het niveau van de straten.
Ces statistiques seront vérifiées et validées par l'Organe de contrôle de l'information policière. Dès que cet Organe aura validé ces statistiques, elles seront transmises à la NTSU (National Technical & Tactical Support Unit) qui indiquera à l'aide d'une carte aux opérateurs quels arrondissements/zones de police sont soumis à la conservation de données ainsi que la durée de conservation.	Deze statistieken zullen worden gecontroleerd door het Controleorgaan op de politionele informatie. Zodra deze instantie deze statistieken heeft gevalideerd, zullen zij worden toegezonden aan de NTSU (National Technical & Tactical Support Unit)), die de operatoren door middel van een kaart zal aangeven voor welke gemeenten/politiezones gegevens worden bewaard en voor hoe lang.
Le deuxième critère porte sur le niveau de la menace terroriste ou extrémiste (échelle de 1 à 4, variant de faible à très grave).	Het tweede criterium heeft betrekking op het dreigingsniveau inzake terrorisme of extremisme (schaal van 1 tot 4, gaande van laag naar zeer ernstig).
Il s'agit, dans cette hypothèse, de réaliser une conservation générale ou ciblée, des données visées au § 2, au sens où, ces données ne sont traitées que lorsque et aussi longtemps que le niveau de la menace terroriste et extrémiste sur ce lieux atteint un niveau 3. Dès lors qu'un niveau de la menace atteint le niveau 3 (menace possible et vraisemblable) et, a fortiori, 4 (menace sérieuse et imminente), une conservation des données visées au § 2 sur les zones géographiques visées est réalisée. Il peut dans certains cas (évaluation générale de la menace de niveau 3 ou 4) s'agir de l'ensemble du territoire.	Wanneer het algemene dreigingsniveau voor terrorisme en extremisme in ons land op niveau 3 of hoger wordt ingeschaald, wordt een algemene bewaarplicht ingesteld van de gegevens bedoeld in §2. De bewaring is gericht, in de zin dat de bewaring geldt zolang het dreigingsniveau op 3 (dreiging mogelijk en waarschijnlijk) of op 4 (dreiging ernstig en zeer nabij) wordt ingeschaald. In deze gevallen wordt een algemene en ongedifferentieerde dataretentie opgelegd over heel het grondgebied.
Dans ce dernier cas, dès lors que la menace en matière de terrorisme ou d'extrémisme est grave ou très grave, il est nécessaire d'activer une conservation de données pour l'ensemble du territoire et ce, aussi longtemps que le niveau 3 ou le niveau 4 perdure. En effet même si une évaluation passe du niveau 4 vers le niveau 3, une	Met andere woorden, zodra de dreiging van terrorisme of extremisme ernstig of zeer ernstig is, is het noodzakelijk om de gegevensbewaring voor het gehele grondgebied te activeren, zolang de dreiging niveau 3 of niveau 4 blijft. Immers, zelfs indien een evaluatie van niveau 4 naar niveau 3 gaat, moet de bewaring algemeen

conservation généralisée et indifférenciée doit être maintenue pour faire face à la menace qui reste réelle et actuelle.	en ongedifferentieerd blijven om het hoofd te kunnen bieden aan de dreiging die reëel en actueel blijft.
Ce niveau de la menace 3 ou 4 est établi par un Organe indépendant des services qui utilisent les données des opérateurs	Dit niveau van bedreiging 3 of 4 wordt vastgesteld door een instantie die onafhankelijk is van de diensten die de gegevens van de exploitanten gebruiken
Dans la pratique, l'Organe de Coordination pour l'Analyse de la Menace (OCAM) reçoit les informations permettant de faire les analyses générale ou spécifique. Ces données proviennent des différents services d'appui. L'OCAM détermine de manière indépendante le niveau de la menace visé à l'article 8 de sa loi organique (Loi du 10 juillet 2006 relative à l'analyse de la menace).	In de praktijk ontvangt het coördinatieorgaan voor dreigingsanalyse (OCAD) voor haar analyse van de verschillende ondersteunende diensten. Het OCAD beslist zelfstandig over het dreigingsniveau zoals bedoeld in artikel 8 van haar organieke wet (wet van 10 juli 2006 betreffende de dreigingsanalyse).
Bien entendu, l'OCAM doit, sur la base des informations reçues par les services d'appui revoir in concreto, le niveau de la menace. En pratique, cette évaluation a lieu une fois par mois.	Uiteraard moet het OCAD, op basis van de door de ondersteunende diensten ontvangen informatie, het niveau van de dreiging in concreto herevalueren. In de praktijk wordt één keer per maand een evaluatie gemaakt.
La conservation des données de localisation et de trafic dans les zones stratégiques (§ 3 points 3 à 5)	Bewaring van verkeers- en locatiegegevens op basis van strategische zones (§ 3, punten 3 tot 5)
Les points 3 à 5 du paragraphe 3 sont aussi entièrement nouveaux et traitent de la limitation de l'obligation de conservation sur la base de critères géographiques. La Cour de justice de l'Union européenne a jugé qu'une mesure prévoyant la conservation de données relatives au trafic et de données de localisation peut être définie sur la base d'un critère géographique, notamment s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave, ou que ces zones peuvent être la cible de menaces graves contre la sécurité publique.	De punten 3 tot 5 van paragraaf 3 zijn eveneens nieuw en hebben betrekking op de beperking van de bewaarplicht op basis van geografische criteria. Het Europees Hof van Justitie heeft geoordeeld dat een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens kan worden ingesteld op basis geografische criterium, met name indien op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat in een of meer geografische gebieden een groot risico bestaat op het voorbereiden of plegen van ernstige criminaliteit, of dat er plaatsen zijn waar de bewaring van gegevens als preventieve maatregel noodzakelijk is omdat zij het doelwit kunnen zijn van ernstige bedreigingen van de openbare veiligheid.
Ce risque s'analyse notamment en terme de probabilité ou d'impact. Vu le caractère stratégique des zones reprises dans ces points, l'impact des actes de criminalité est d'office élevé.	Dit risico wordt geanalyseerd in termen van waarschijnlijkheid of impact. Gezien het strategische karakter van de zones die onder deze punten vallen, is de impact van criminele daden automatisch groot.

<p>Le paragraphe 3 énumère d'une part, les critères génériques qui peuvent être pris en compte dans la détermination des zones géographiques et mentionne d'autre part, les zones géographiques qui répondent à ces critères tout en laissant par ailleurs au Roi, par arrêté délibéré en Conseil des Ministres, la possibilité d'ajouter d'autres lieux stratégiques qui correspondent à ces critères. Il est d'emblée important de souligner que l'article en projet reprend les critères explicitement mentionnés par la Cour de justice tels que les lieux fréquentés par un grand nombre de personnes ou les lieux stratégiques, tels que les aéroports, les gares ferroviaires ou les gares de péage (§ 150 de l'arrêt du 6 octobre 2020). Ces critères sont précisés dans le présent article.</p>	<p>Paragraaf 4 somt de algemene criteria op die in aanmerking kunnen worden genomen bij de bepaling van de geografische gebieden en vermeldt de geografische gebieden die aan deze criteria voldoen. De Koning kan hiernaast, bij een in Ministerraad overlegd besluit, andere strategische locaties die aan deze criteria voldoen, toevoegen. Dit ontwerp-artikel herneemt letterlijk de door het Europees Hof van Justitie uitdrukkelijk genoemde criteria, zoals plaatsen die door een groot aantal mensen worden bezocht of strategische locaties, zoals luchthavens, spoorwegstations of tolstations (§ 150 van het arrest van 6 oktober 2020). Deze criteria worden in dit artikel nader omschreven.</p>
<p>Un seul critère est nécessaire pour établir qu'il faille à titre préventif réaliser une conservation de données sur un lieu.</p>	<p>Een plaats moet aan minstens één criterium voldoen om vast te stellen dat de bewaring van gegevens noodzakelijk is als preventieve maatregel.</p>
<p>Il faut d'emblée noter que, dès lors qu'un lieu est affecté à d'autres destinations, la conservation à titre préventif des données de trafic et de localisation sur ce lieu à titre de lieu stratégique (X) s'arrête, sauf, bien entendu s'il peut toujours constituer un autre lieu stratégique (Y). C'est d'ailleurs dans cette optique qu'il est stipulé que les autorités compétente informent sans délai le NTSU des modifications de la destination des lieux.</p>	<p>Er dient onmiddellijk te worden opgemerkt dat, zodra een locatie een andere bestemming krijgt, de bewaring van verkeers- en locatiegegevens over deze locatie als strategische locatie (X) ophoudt, tenzij het door haar aard parallel ook nog een andere strategische locatie (Y) is. In dit verband is bepaald dat de bevoegde autoriteiten de NTSU in kennis moeten stellen van bestemmingswijzigingen van de plaatsen.</p>
<p>Les lieux suivants sont repris comme critère permettant de réaliser une conservation de données de trafic et de localisation car ils constituent des zones particulièrement exposées à la commission d'actes de criminalité grave ou parce qu'ils sont exposés à des menaces pour la sécurité nationale :</p>	<p>De volgende plaatsen zijn opgenomen als criterium voor de bewaring van verkeers- en locatiegegevens omdat het zones zijn die bijzonder vatbaar zijn voor het plegen van zware criminaliteit of omdat zij blootstaan aan bedreigingen van de nationale veiligheid:</p>
<ul style="list-style-type: none"> - les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation; les gares ferroviaires , les stations de métro et de pré-métro; les aéroports: <p>Les lieux où il y a un transport de passagers sont effet susceptibles d'être la cible d'actes</p>	<ul style="list-style-type: none"> - de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek, treinstations, metro- en pre-metrostations; luchthavens: <p>Plaatsen waar personenvervoer plaatsvindt, kunnen immers het doelwit zijn van criminele</p>

<p>de criminalité grave comme les attentats de Bruxelles en 2016 l'ont démontré (attentat à l'aéroport de Zaventem et à la station de métro de Maelbeek). Les aéroports et les ports sont bien entendu aussi des lieux où, par exemple, le trafic des êtres humains est organisé, ou encore l'import de stupéfiants. Il est certain à cet égard que ce n'est pas uniquement les grands aéroports/ports qui doivent être visés puisque, précisément dans le but de tenter d'échapper à un contrôle, des ports et des aéroports plus modestes sont parfois choisis comme zone pour commettre des infractions graves, par les organisations criminelles.</p>	<p>handelingen, zoals de aanslagen in Brussel in 2016 hebben aangetoond (aanslag op de luchthaven van Zaventem en het metrostation van Maelbeek). Luchthavens en havens zijn natuurlijk ook plaatsen waar mensenhandel wordt georganiseerd, of nog de invoer van drugs. Het is duidelijk dat in dit verband niet alleen grote luchthavens/havens moeten worden aangepakt, want juist in een poging om aan de controle te ontsnappen, worden kleinere havens en luchthavens soms gekozen door criminele organisaties.</p>
<ul style="list-style-type: none"> - L'ensemble des juridictions et les bâtiments de l'ordre judiciaire : dans le cadre de la tenue de procès, ces lieux constituent l'objet de menaces. Pour prévenir ces menaces ou enquêter, une conservation de données sur ces lieux est nécessaire, et ce, même en dehors de la tenue d'un procès, vu que ces lieux symbolisent la Justice et sont donc susceptibles de faire l'objet d'actes de criminalité grave. ce point ne vise pas uniquement les juridictions de l'ordre judiciaire dans la mesure où les autres bâtiments qui accueillent du personnel de l'ordre judiciaire sont également susceptibles d'être la cible d'attentats. 	<ul style="list-style-type: none"> - De hoven en rechtbanken en de gebouwen van de rechterlijke macht: in het kader van de procesvoering zijn deze plaatsen blootgesteld aan dreigingen. Om deze dreigingen te voorkomen of om onderzoek te voeren, is het noodzakelijk gegevens over deze plaatsen bij te houden, zelfs buiten het kader van een proces, aangezien deze plaatsen symbool staan voor justitie en dus het voorwerp kunnen zijn van ernstige criminaliteit. Het is niet voldoende om enkel de hoven en rechtbanken als mogelijk doelwit te harnemen, aangezien ook andere gebouwen waarin justitieel personeel is gehuisvest, vatbaar zijn voor aanslagen.
<ul style="list-style-type: none"> - Les bâtiments de la police fédérale et de la police locale : Il s'agit en effet de lieux qui, d'une part, représentent la puissance publique de l'Etat et, d'autre part, dans lesquels des armes et munitions, des uniformes ou des biens saisis dont notamment de la drogue, sont stockés. Du matériel technologique spécifique est aussi stocké dans certaines unités de police. A ces titres, ils peuvent bien entendu constituer la cible d'attentat, d'actes de violence ou de vols, comme cela a déjà été le cas par le passé (poste de police de Verviers et Charleroi). 	<ul style="list-style-type: none"> - De gebouwen van de Federale en lokale politie: Dit zijn plaatsen die de openbare macht van de Staat vertegenwoordigen en waar wapens en munitie of in beslag genomen goederen, met inbegrip van drugs, worden opgeslagen. Specifiek technologisch materiaal is eveneens opgeslagen bij bepaalde politie-eenheden. Als zodanig kunnen zij uiteraard het doelwit van aanslagen zijn, zoals in het verleden reeds het geval is geweest (politiebureaus van Verviers en Charleroi).
<ul style="list-style-type: none"> - Les bâtiments de l'administration des douanes et accises. Il s'agit de bâtiments dans lesquels des biens saisis sont entreposés. Il peut s'agir de quantité 	<ul style="list-style-type: none"> - De gebouwen van de administratie Douane en Accijnzen. Dit zijn gebouwen waar in beslag genomen goederen worden opgeslagen. Het kan soms gaan om grote hoeveelheden drugs, wapens

parfois élevée de drogues, d'armes ou des biens de valeur. Ces lieux sont dès lors particulièrement exposés à la commission d'actes de criminalité grave.	of waardevolle goederen. Deze plaatsen zijn derhalve bijzonder kwetsbaar voor het plegen van zware criminaliteit.
<ul style="list-style-type: none"> - Les communes où il y a des domaines militaires : Les domaines militaire sont des zones particulièrement exposées à des menaces pour la sécurité nationale et à la commission d'actes de criminalité grave. En effet, sont stockés dans les domaines militaires des armes, des munitions, des explosifs, des systèmes d'armes, du matériel à haut potentiel technologique, du matériel, des documents et des systèmes informatiques classifiés, du matériel pour assurer la sécurité aérienne, ... Ces éléments font l'objet de convoitise de la part notamment de certains mouvements extrémistes et de services de renseignement étrangers. Seules les communes seront communiquées et pas les sites précis. Ceci s'explique par la sensibilité des quartiers militaires. En effet, nombreux sont classifiés. Il n'est donc pas envisageable de donner un point précis sur une carte à tous les opérateurs. Pour rappel, l'article 120ter du Code pénal punit quiconque fera des photos dans un rayon de 10km autour d'établissements militaires. Vu ce caractère sensible, couvrir les communes dans lesquelles se trouvent des domaines militaires est proportionné. 	<ul style="list-style-type: none"> - Gemeenten waar zich militaire domeinen bevinden: Militaire domeinen zijn gebieden die in het bijzonder blootstaan aan bedreigingen voor de nationale veiligheid en aan het plegen van ernstige strafbare feiten. Wapens, munitie, explosieven, wapensystemen, uitrusting met een hoog technologisch potentieel, geclassificeerd materiaal, documenten en computersystemen, uitrusting voor het waarborgen van de veiligheid van het luchtverkeer, enz. liggen namelijk opgeslagen in militaire zones. Deze elementen zijn begeerd door bepaalde extremistische bewegingen en buitenlandse inlichtingendiensten. Alleen de gemeenten zullen worden meegedeeld en niet de precieze locaties. Dit is te wijten aan de gevoeligheid van militaire kwartieren. Inderdaad, velen van hen zijn geclassificeerd. Het is dus niet mogelijk om alle exploitanten een precies punt op een kaart te geven. Ter herinnering: artikel 120ter van het Wetboek van Strafrecht stelt eenieder strafbaar die foto's neemt binnen een straal van 10 km van militaire inrichtingen. Gezien deze gevoelige aard is het evenredig de gemeenten waarin zich militaire domeinen bevinden, in het toepassingsgebied op te nemen.
<ul style="list-style-type: none"> - Les prisons et les maisons de transition: ces lieux représentent aussi un risque élevé au niveau de préparation d'actes d'évasion et parfois de trafic et de consommation de stupéfiant. 	<ul style="list-style-type: none"> - De gevangenissen en transitiehuizen: deze plaatsen vormen ook een verhoogd risico wat betreft (de voorbereiding van) ontsnappingen, drugshandel en -gebruik.
<ul style="list-style-type: none"> - Les armuriers et les centres de tir: vu que ces lieux concentrent une quantité d'armes et de munitions, il est nécessaire de faire une data retention sur ces lieux. 	<ul style="list-style-type: none"> - Wapenkamers en schietcentra: aangezien op deze plaatsen een hoeveelheid wapens en munitie wordt geconcentreerd, is het noodzakelijk gegevens over deze plaatsen te bewaren.
Par ailleurs, le législateur a lui-même identifié à travers différent(e)s lois ou arrêtés royaux ces lieux stratégiques qui doivent faire l'objet d'une attention et d'une	De wetgever heeft zelf, door middel van verschillende wetten of koninklijke besluiten, deze strategische locaties aangewezen die speciale aandacht en bescherming moeten

protection particulières car une atteinte à ces lieux auraient d'office une répercussion majeure au niveau de la sécurité nationale et parce qu'elles sont exposées à des risques élevés de criminalité grave	krijgen, omdat een aanval op deze locaties automatisch grote gevolgen zou hebben voor de nationale veiligheid.
- Il s'agit premièrement des sites nucléaires. Une attaque sur un site nucléaire constituerait en soi un incident grave qui nécessite le déclenchement de plans d'urgence, notamment pour porter secours à la population. En fonction de l'ampleur des dégâts, les intérêts vitaux de la population peuvent être touchés.	- Ten eerste , zijn er de nucleaire sites. Een aanval op een nucleaire site zou op zich een ernstig incident vormen dat de activering van noodplannen vereist, met name om de bevolking te redden. Afhankelijk van de omvang van de schade kunnen de vitale belangen van de bevolking worden aangetast.
- Deuxièmement , vu les activités liées à la manipulation, la fabrication, l'emploi ou le stockage de substances dangereuses, les entreprises SEVESO peuvent, bien entendu, elles aussi constituer une cible 'privilégiée' d'attentats ou d'actes malveillants. Une attentat sur un tel site constitue immédiatement une menace grave pour la sécurité nationale.	- Ten tweede kunnen de SEVESO-bedrijven, gezien hun activiteiten gelieerd aan de behandeling, de productie, het gebruik of de opslag van gevaarlijke stoffen, ook een "geprivilegieerd" doelwit vormen voor aanslagen of kwaadwillige handelingen. Een aanslag op zo'n site vormt onmiddellijk een ernstige bedreiging voor de nationale veiligheid.
- Il s'agit troisièmement des infrastructures critiques telles que visées à l'article 1 ^{er} la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques. Vu le lien entre ces infrastructures critiques et la production et les transports vitaux d'énergie, les points de jonction vitaux des transports, les maillons indispensables des systèmes de paiement électronique et des réseaux de communications électroniques, une atteinte à celles-ci constitue ipso facto une menace pour la sécurité nationale.	- Ten derde de kritieke infrastructuur zoals bedoeld in artikel 1 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur. Door het verband tussen deze kritieke infrastructuur en vitale energieproductie en -vervoer, vitale verkeersknooppunten, onmisbare schakels in elektronische betalingssystemen en elektronische communicatienetwerken, vormt een inbreuk hierop ipso facto een bedreiging voor de nationale veiligheid.
Comme les adresses spécifiques des infrastructures critiques font l'objet d'une classification au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, elles ne peuvent pas en tant que telles être communiquées aux opérateurs. Par contre les communes qui hébergent ces infrastructures critiques font l'objet d'une diffusion restreinte et peuvent dès lors sur la base du principe du besoin d'en connaître être communiquées aux opérateurs via le service désigné par le Roi, soit le service NTSU.	Aangezien de specifieke adressen van kritieke infrastructuur geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, kunnen zij niet als zodanig aan de operatoren worden meegedeeld. De gemeenten waar deze kritieke infrastructuur zich bevinden zijn echter onderworpen aan een behandeling op niveau "beperkte verspreiding" en kunnen zij dus, op basis van het "need-to-know"-beginsel, aan de operatoren worden meegedeeld via de door de Koning aangewezen dienst, namelijk de NTSU.
- Quatrièmement , les infrastructures des opérateurs étatiques qui assurent les	- Ten vierde moeten de infrastructuur van staatsbedrijven die de communicatie in

communications en situation de crise telles les réseaux Astrid ou Binii, doivent, comme l'intitulé le mentionne, offrir en cas de crise, une possibilité pour l'Etat de maintenir une communication de crise. Si ces infrastructures sont touchées, il n'y a potentiellement plus de communication étatique de crise, ce qui a immédiatement une répercussion grave au niveau de la sécurité nationale.	crisissituaties waarborgen, zoals het Astrid- of het Binii-netwerk, de staat, zoals de titel vermeldt, de mogelijkheid bieden om de crisiscommunicatie in crisissituaties in stand te houden. Indien deze infrastructures worden aangetast, is er potentieel geen crisiscommunicatie van de staat meer mogelijk, hetgeen onmiddellijk ernstige gevolgen heeft voor de nationale veiligheid.
- Enfin, les réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de service essentiels constituent eux aussi des 'lieux cybers' qui peuvent faire l'objet d'attaque ciblée lesquelles auraient une répercussion sur la sécurité nationale.	- Ten slotte , de informatienetwerken en – systemen die de verlening van essentiële diensten van operatoren van essentiële diensten ondersteunen , zijn ook "cyberplaatsen" die het voorwerp kunnen zijn van gerichte aanvallen die gevolgen zouden hebben voor de nationale veiligheid.
- Un autre critère qui permet de réaliser une conservation préalable des données de trafic et de localisation concerne la menace grave potentielle au sein de la zone pour les intérêts vitaux du pays ou les besoins essentiels de la population.	- Een ander criterium betreft de mogelijke ernstige bedreiging binnen het gebied voor de vitale belangen van het land of de essentiële behoeften van de bevolking.
Ce que l'on entend par intérêts vitaux ou besoins essentiels est subdivisé en 6 catégories, dont 4 sont extraites du plan d'urgence cybernétique : l'ordre public, le potentiel scientifique et économique du pays, la souveraineté nationale et les institutions établies par la Constitution et les lois, et l'intégrité du territoire national. La cinquième catégorie est le transport et la sixième, reprise de l'article 23.1.e du GDPR 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.	Wat wordt verstaan onder vitale belangen of essentiële behoeften is onderverdeeld in zes categorieën, waarvan er vier zijn overgenomen uit het cybernoodplan: de openbare orde, het wetenschappelijk en economisch potentieel van het land, de nationale soevereiniteit en de bij de grondwet en de wetten opgerichte instellingen, en de integriteit van het nationale grondgebied. De vijfde categorie is het transport en de zesde, overgenomen uit artikel 23.1.e van de AVG behelst de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid
La potentialité de la menace désigne des dangers dont l'existence n'est pas au moment où elle est appréhendée, établie ou dont la probabilité n'est pas encore démontrée.	De mogelijkheid van de dreiging heeft betrekking op gevaren waarvan het bestaan nog niet is vastgesteld of waarvan de waarschijnlijkheid nog niet is aangetoond
Au niveau de l'ordre public, deux catégories de zone sont déterminées dans l'article en projet. Il s'agit des zones neutres (ex zone neutre de Bruxelles) soit le périmètre au	Wat de openbare orde betreft, worden in het ontwerp-artikel twee categorieën van zones bepaald. Dit is de neutrale zone in Brussel, d.w.z. de zone waarbinnen betogingen

sein duquel il est interdit de manifester et des cabinets ministériels. Vu que ces zones englobent les lieux de pouvoir, la violation de ces zones entraîne un risque élevé que certaines structures de pouvoir ne puissent plus se réunir et prendre les mesures adéquates.	verboden zijn en de ministeriële kabinetten. Aangezien deze zones de machtscentra omvatten, houdt de schending van deze zones een groot risico in dat bepaalde machtsstructuren niet meer kunnen vergaderen en geen passende maatregelen meer kunnen nemen.
En termes de potentiel scientifique et économique, la menace est, par exemple, automatiquement grave lorsqu'elle concerne la recherche universitaire ou scientifique dans les vastes domaines de la micro- et de la nanoélectronique, de la biotechnologie et de la technologie à large bande. Il s'agit donc notamment des "centres de recherche stratégiques" reconnus par la Région flamande et des "centres de recherches agréées" reconnus par la Région wallonne.	Wat betreft het wetenschappelijk en economisch potentieel is de dreiging bijvoorbeeld automatisch ernstig wanneer zij betrekking heeft op academisch of wetenschappelijk onderzoek op de brede wetenschapsdomeinen van micro- en nano-elektronica, biotechnologie en breedbandtechnologie. Daardoor worden hiermee de "strategische onderzoekscentra" bedoeld zoals erkend door het Vlaams gewest, alsook de "centres de recherches agréées" zoals erkend door het Waals Gewest.
La liste des personnes morales belges dont le potentiel économique et/ou scientifique doit être protégé est établie par les 2 services PES (potentiel économique et scientifique) des services de renseignement lesquels, sur la base de leur loi organique, ont comme mission la protection du potentiel scientifique et économique du pays (articles 7, 1 ^{er} et 11, §1 ^{er} , c) de la loi organique des services de renseignement et de sécurité).	De lijst van de Belgische rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel moet worden beschermd, wordt opgesteld door de twee diensten EWP (economisch en wetenschappelijk potentieel) van de inlichtingendiensten die, op grond van hun organieke wet, tot taak hebben het wetenschappelijk en economisch potentieel van het land te beschermen (artikelen 7, 1 ^o en 11, §1, c) van de organieke wet inzake de inlichtingen- en veiligheidsdiensten).
Cette liste est établie annuellement par la Sûreté de l'Etat et le Service général du Renseignement et de la sécurité sur proposition des Ministres de la Justice et de la Défense et approuvée par le Conseil national de sécurité.	Deze lijst wordt opgesteld door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid op voorstel van de ministers van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad.
En ce qui concerne les transports, les autoroutes constituent un réseau de transport essentiel de notre pays, grâce auquel l'approvisionnement doit pouvoir être assuré en cas d'urgence.	Wat betreft het transport vormen de autosnelwegen een essentiële netwerk van transport in ons land, waarlangs de bevoorrading in noodsituaties moet kunnen verzekerd worden.
Au niveau de la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances, l'ensemble des lieux suivants peuvent faire l'objet d'une menace potentielle et grave. La menace est d'office grave lorsqu'elle touche les lieux qui symbolisent la souveraineté	Wat betreft de nationale soevereiniteit en de instellingen die bij de grondwet en wetten, decreten of verordeningen zijn opgericht, kunnen alle volgende plaatsen aan een potentiële en ernstige bedreiging worden blootgesteld. De dreiging is automatisch ernstig wanneer zij plaatsen treft die

<p>nationale et les institutions établies par la Constitution ou les lois, décrets ou ordonnances.</p>	<p>symbool staan voor de nationale soevereiniteit en de instellingen die zijn opgericht bij de grondwet of bij wetten, decreten of verordeningen.</p>
<p>Il s'agit premièrement des différents parlements du pays et qui sont visés au chapitre II et IV de la Constitution. A ce titre, il s'agit aussi de protéger les assemblées législatives au niveau communal et provincial. En effet, il s'agit d'offrir une protection uniforme à tous les élus qui représente la nation.</p>	<p>Dit zijn in de eerste plaats de verschillende parlementen van het land waarnaar in de hoofdstukken II en IV van de Grondwet wordt verwezen. In dit verband gaat het er ook om de wetgevende vergaderingen op gemeentelijk niveau te beschermen. Het gaat er immers om alle verkozen vertegenwoordigers van de natie een uniforme bescherming te bieden.</p>
<p>Il s'agit deuxièmement de protéger le Roi et donc concrètement de permettre de réaliser une conservation de données de trafic et de localisation près du palais royal et des domaines royaux qui font d'ailleurs l'objet d'autres protections spécifiques.</p>	<p>In de tweede plaats gaat het om de bescherming van de koning en gaat het er dus concreet om verkeers- en locatiegegevens op te slaan in de buurt van het koninklijk paleis en de koninklijke domeinen, die ook een andere specifieke bescherming genieten.</p>
<p>Il s'agit troisièmement d'apporter une protection d'une part aux bâtiments du pouvoir judiciaire, soit aux cours et tribunaux du pouvoir judiciaire visé au chapitre VI de la Constitution et au Conseil d'Etat visées au chapitre VII de la Constitution.</p>	<p>Ten derde gaat het om de bescherming van de gebouwen van de rechterlijke macht, d.w.z. de rechtbanken en gerechtshoven van de rechterlijke macht bedoeld in hoofdstuk VI van de Grondwet en de Raad van State bedoeld in hoofdstuk VII van de Grondwet.</p>
<p>Il s'agit aussi des protéger les corps qui représentent la force publique au sens du titre VI de la Constitution, soit la police et les militaires. Comme il s'agit de protéger des lieux avec une menace grave et potentielle, la protection porte respectivement sur les postes de police et les domaines militaires.</p>	<p>Tenslotte gaat het om de bescherming van de organen die de openbare macht vertegenwoordigen in de zin van Titel VI van de Grondwet, namelijk de politie en het leger. Aangezien het gaat om de bescherming van plaatsen met een ernstige en potentiële dreiging, betreft de bescherming respectievelijk politiebureaus en militaire domeinen.</p>
<p>Au niveau de l'intégrité du territoire national, les communes frontalières doivent être soumises à une 'data retention'. En cas d'attaque ou d'invasion ces communes constituent des lieux stratégiques pour la souveraineté nationale. Les communes frontalières ont été retenues comme zones géographiques dans la conservation ciblée, étant donné que la pratique montre que des groupes d'individus (bandes urbaines, organisations criminelles, etc.) venant de l'étranger commettent des infractions pénales en Belgique comme l'organisation de trafic de stupéfiants, des coups et blessures, vols de voiture et conduite</p>	<p>Wat de nationale territoriale integriteit betreft, zijn de grensgemeenten onderworpen aan de verplichting gegevens te bewaren. In geval van een aanval of invasie zijn deze gemeentes van strategisch belang voor de nationale soevereiniteit. De grensgemeenten zijn in de gerichte bewaring in aanmerking genomen als geografische gebieden aangezien uit de praktijk blijkt dat groepen van individuen (stadsbendes, criminele organisaties, enz.) vanuit het buitenland in België strafbare feiten komen plegen, zoals de organisatie van drugshandel, slagen en verwondingen, autodiefstal en gevaarlijk rijden ("joyriding")</p>

dangereuse (« joy riding ») et que des groupes d'individus résidant en Belgique passent la frontière pour commettre de telles infractions.	en dat groepen van individuen die in België verblijven de grens oversteken om daar zulke inbreuken te plegen.
Enfin, dans le domaine de la santé, les hôpitaux et dans le domaine économique et financier, la BNB sont des zones vitales pour les besoins essentiels de la population. Un hacking des hôpitaux par exemple constituerait une menace grave pour ces intérêts.	Ten slotte zijn in de gezondheidssector, de ziekenhuizen en in de economische en financiële sector, de NBB van vitaal belang voor de basisbehoeften van de bevolking. Het hacken van ziekenhuizen, bijvoorbeeld, zou een ernstige bedreiging voor deze belangen vormen.
Carte transmise aux opérateurs par le service NTSU pour identifier les zones soumises à une conservation de données à titre préventif	Kaart die door de NTSU-dienst aan de operatoren wordt toegezonden om de zones aan te duiden waarvoor preventieve gegevensbewaring geldt
Les lieux ou catégories de lieux visés dans la loi (§ 3 point 1° à 5°) et, le cas échéant, dans l'Arrêté royal sont reportés sur une carte par la NTSU au moins une fois par an. Cette carte, ainsi que, le cas échéant, les délais de conservation spécifique, seront transmis par le service NTSU aux opérateurs pour qu'ils puissent, en pratique, respecter l'obligation de conservation ciblée que la loi leur impose.	De in de wet (§ 3, punten 1° tot 5°) en, desgevallend in het koninklijk besluit, bedoelde plaatsen of categorieën van plaatsen worden minstens eenmaal per jaar door de NTSU in kaart gebracht. Deze kaart en eventuele specifieke bewaartermijnen zullen aan de operatoren worden verzonden, zodat zij in de praktijk de verplichting tot gerichte bewaring kunnen nakomen die de wet hun oplegt.
Tant les lieux précisés dans la loi que ceux indiqués dans l'Arrêté royal doivent être aussi précis que possible, ne laissant à la NTSU aucune marge d'appréciation. De cette manière, la carte sur laquelle ces lieux seront reportés est un simple acte matériel d'exécution, sans contenu juridique propre. Cette carte ne doit donc pas être publiée.	Zowel de in de wet als de in het koninklijk besluit genoemde plaatsen moeten zo nauwkeurig zijn, dat de NTSU geen beoordelingsmarge heeft. Zo is de kaart waarop deze plaatsen zullen worden ingevuld een louter materiële uitvoeringshandeling, zonder eigen juridische inhoud. De kaart hoeft dus niet te worden gepubliceerd.
Ceci dit, le fait que les catégories de zones géographiques doivent être déterminées de manière précise et objective, n'implique pas que la loi ou l'Arrêté royal identifie très précisément quels sont les lieux répondant à ces catégories. C'est notamment le cas pour le critère relatif aux statistiques. Cette catégorie est précise et objective, mais il est indispensable de disposer de statistiques, qui ne sont pas publiques, à ce sujet, pour déterminer quelles sont concrètement les communes visées. La recherche de ces statistiques n'implique toutefois aucun pouvoir d'appréciation. Il s'agit seulement de recueillir et d'appliquer des données pertinentes.	Dat de categorieën van geografische gebieden op precieze en objectieve wijze moeten worden vastgesteld, impliceert evenwel niet dat de wet of het koninklijk besluit zeer nauwkeurig vaststelt welke plaatsen onder deze verschillende categorieën vallen. Dit is met name het geval voor het criterium inzake statistieken. Deze categorie is nauwkeurig en objectief, maar het is van essentieel belang over statistieken te beschikken, die niet noodzakelijk openbaar zijn, om te kunnen bepalen welke gemeenten daadwerkelijk onder de regeling vallen. Het zoeken naar dergelijke statistieken impliceert evenwel geen discretionaire bevoegdheid. Het is alleen

	een kwestie van relevante gegevens te verzamelen en toe te passen.
En pratique, ce sera le service NTSU de la police fédérale qui transmettra au moins annuellement la carte aux opérateurs. Ce service est déjà le canal de communication entre les autorités requérantes (autorités judiciaires, services de renseignements, etc.) et les opérateurs qui doivent effectuer les réquisitions.	In de praktijk zal het de dienst NTSU van de federale politie zijn die minstens jaarlijks de kaart aan de operatoren zal overmaken. Deze dienst is reeds het communicatiekanaal tussen de verzoekende autoriteiten (gerechtelijke autoriteiten, inlichtingendiensten, enz.) en de operatoren die de opvorderingen moeten doen.
Concrètement, c'est ce service qui, sur la base des critères fixés par la loi et des lieux qui y sont énumérés, ainsi que ceux éventuellement mentionnés dans l'Arrêté royal, établira la carte des lieux spécifiques dans lesquels s'applique l'obligation de conservation des données par les opérateurs.	Concreet is het deze dienst die, op basis van de door de wet vastgestelde criteria en de daarin opgesomde plaatsen, alsmede de plaatsen die eventueel in het Koninklijk Besluit worden vermeld, de kaart zal opstellen van de specifieke plaatsen waar de verplichting tot het bewaren van gegevens door de marktdeelnemers geldt.
Afin que le service NTSU puisse exécuter ses missions, chaque autorité compétence devra transmettre à échéance déterminée par le Roi les données opérationnelles nécessaires pour réaliser la carte. Cependant dès qu'une zone change de finalité (destination), cette autorité a aussi l'obligation de communiquer ce changement sans délai au NTSU.	Opdat de NTSU-dienst zijn taken kan uitvoeren, moet elke bevoegde autoriteit de operationele gegevens die nodig zijn om de kaart op te stellen, vóór een door de Koning vastgestelde datum indienen. Zodra een gebied echter zijn bestemming wijzigt, is deze autoriteit ook verplicht deze wijziging onverwijld aan de NTSU mee te delen.
Il faut noter que selon la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, l'IBPT est chargé du contrôle du respect entre autres de la loi télécom. Cette compétence générale de contrôle n'implique cependant pas que l'IBPT soit amené à contrôler le respect des obligations que l'article 126/1 met à charge des autorités.	Er zij op gewezen dat volgens de wet van 17 januari 2003 betreffende het statuut van de regulator van de Belgische post- en telecommunicatiesector, het BIPT belast is met het toezicht op de naleving van onder meer de telecomwet. Deze algemene controlebevoegdheid houdt evenwel niet in dat het BIPT moet controleren of de verplichtingen die artikel 126/1 aan de autoriteiten oplegt, worden nageleefd
Il est également précisé que, sauf pour ce qui concerne les statistiques de criminalité, la loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article. En effet, il faut éviter qu'il soit demandé aux autorités compétentes de divulguer ou d'autoriser la	Verder wordt ook bepaald dat, behalve wat de criminaliteitsstatistieken betreft, de wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie niet van toepassing zijn op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel. Er moet inderdaad voorkomen worden dat aan de bevoegde autoriteiten gevraagd wordt om de

consultation des données opérationnelles qu'elles mettent à la disposition du service NTSU. Ces autorités seront dans de nombreux cas des autorités administratives. Bien que les lois en question prévoient certaines exceptions au cas par cas, le gouvernement estime que les données en question sont si sensibles qu'un régime d'exception général est justifié.	operationele gegevens die zij ter beschikking stellen van de dienst NTSU openbaar te maken of te laten consulteren. Deze autoriteiten zullen in veel gevallen administratieve overheden zijn. Hoewel de wetten in kwestie bepaalde uitzonderingen voorzien op een case-by-case basis, is de regering van mening dat de bedoelde gegevens zo gevoelig zijn dat een algemeen uitzonderingsregime gerechtvaardigd is.
Evaluation de la loi et de l'arrêté royal	Evaluatie van de wet en van het koninklijk besluit
Après l'avis du Comité de coordination du Renseignement et de la Sécurité (CCRS) et des autorités de protection des données compétentes, les ministres compétents établiront un rapport qui sera soumis à la Chambre des représentants. L'objet de ce rapport est de vérifier s'il est nécessaire d'adapter les dispositions de la loi ou de l'arrêté royal. Dans le cadre de ce rapportage annuel, il appartient aux ministres compétents de décider de le faire ou non. Une attention particulière sera portée au caractère objectif et non discriminatoire des zones géographiques.	Na het advies van het Coördinatiecomité Inlichtingen en Veiligheid en de bevoegde gegevensbeschermingsautoriteiten, zullen de bevoegde ministers een verslag opmaken dat aan de Kamer van Volksvertegenwoordigers wordt voorgelegd. Het doel van het verslag is na te gaan of het nodig is de bepalingen in de wet of het koninklijk Besluit aan te passen. In het kader van deze jaarlijkse verslaggeving is het aan de bevoegde Ministers om daartoe al dan niet over te gaan. Bijzondere aandacht zal worden besteed aan het objectieve en niet-discriminerende karakter van de geografische gebieden.
Le Comité de coordination est choisi comme organe d'avis car il représente les besoins des services opérationnels en matière d'utilisation des métadonnées de téléphonie.	Het coördinatiecomité is gekozen als adviesorgaan omdat het de behoeften van de operationele diensten bij het gebruik van telefoniemetagegevens vertegenwoordigt.
Composition de ce Comité	Samenstelling van dit comité
Le Comité de coordination pour le renseignement et la sécurité visé par l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du Renseignement et de la Sécurité et du Comité de coordination du Renseignement et de la Sécurité compte les membres permanents suivants : l'administrateur général de la sûreté de l'État, le chef du service général de renseignement et de sécurité des forces armées, le directeur de l'organe de coordination de l'évaluation des menaces, le commissaire général de la police fédérale, le directeur général du centre national de crise du service public fédéral de l'intérieur, le	Het Coördinatiecomité Inlichtingen en de Veiligheid, zoals bedoeld in het Koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid heeft de volgende permanente leden: de administrateur-generaal van de Veiligheid van de Staat, de chef van de Algemene Dienst inlichting en veiligheid van de Krijgsmacht, de directeur van het Coördinatieorgaan voor de dreigingsanalyse, de commissaris-generaal van de Federale Politie, de directeur-generaal van het Nationaal Crisiscentrum van de Federale Overheidsdienst

président du comité exécutif du service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement, un membre du collège des procureurs généraux désigné par le collège, le procureur fédéral et le chef de la défense.	Binnenlandse Zaken, de voorzitter van het directiecomité van de Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, een lid van het College van procureurs-generaal dat door het College wordt aangewezen, de federaal procureur en de Chef Defensie.
C'est la raison pour laquelle le dernier alinéa du paragraphe 5 de cet article prévoit que l'arrêté royal doit être renouvelé tous les trois ans. La période de trois ans semble raisonnable : d'ici là, trois rapportages annuels auront en principe été réalisés, permettant une vision claire des avantages et inconvénients de l'arrêté royal qui aurait été adopté.	Daarom voorziet het laatste lid van paragraaf 4 van dit artikel dat het koninklijk besluit om de drie jaar hernieuwd moet worden. De termijn van drie jaar lijkt redelijk: op dat moment zijn er in principe al drie jaarlijkse evaluaties gedaan, waardoor er een duidelijke visie kan zijn op de verdiensten en de gebreken van het koninklijk besluit dat zou zijn aangenomen. eventuele wijzigingen te implementeren.
Le délai de trois ans n'empêche évidemment pas que l'arrêté royal puisse être révisé plus tôt. En même temps, un renouvellement triennal ne signifie pas nécessairement que le contenu de l'arrêté royal va changer de manière substantielle. Il convient également de rappeler que toute modification de l'arrêté royal doit être soumise à l'Autorité de protection des données pour avis.	De termijn van drie jaar verhindert uiteraard niet dat er vroeger kan herzien worden. Tegelijk betekent een driejaarlijkse hernieuwing niet noodzakelijk dat de inhoud van het koninklijk besluit grondig zal veranderen. Er moet ook rekening gehouden worden met het feit dat elke wijziging van het koninklijk besluit voor advies voorgelegd moet worden aan de Gegevensbeschermingsautoriteit.
Selon le gouvernement, le rapportage annuel avec possibilité de renouvellement de l'arrêté royal, est conforme aux conditions imposées par la Cour de justice.	De jaarlijkse verslaggeving met mogelijkheid tot hernieuwing van het koninklijk besluit, in samenhang met de verplichte driejaarlijkse hernieuwing is volgens de Regering in lijn met wat het Hof van Justitie als voorwaarden oplegt.
Art. 9	Art. 9
Pour une plus grande lisibilité de la loi, le contenu de l'ancien article 127 de la sur les communications électroniques a été transféré vers les articles 127, 127/3 et 127/4 de la même loi.	Om de wet leesbaarder te maken is de inhoud van het oude artikel 127 van de wet op de elektronische communicatie overgebracht naar de artikelen 127, 127/3 et 127/4 van dezelfde wet.
En effet, l'ancien article 127 mélangeait différentes matières que sont l'obligation pour un opérateur d'identifier ses abonnés (dorénavant reprise à l'article 127), la collaboration des opérateurs entre autres avec les autorités judiciaires (dorénavant	Het oude artikel 127 vormde immers een mengeling van verschillende materies, namelijk de verplichting voor een operator om zijn abonnees te identificeren (voortaan opgenomen in artikel 127), de medewerking van de operatoren onder andere met de

reprise à l'article 127/3) et une interdiction qui s'applique à tous de ne pas rendre impossible ou difficile certaines opérations effectuées au bénéfice des autorités, comme l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées (dorénavant reprise à l'article 127/4 de la LCE).	gerechtelijke autoriteiten (voortaan opgenomen in artikel 127/3) en een verbod dat voor iedereen geldt om bepaalde activiteiten uitgevoerd ten behoeve van de autoriteiten, zoals de identificatie van de eindgebruiker, het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privécommunicatie, niet onmogelijk of moeilijk te maken (voortaan opgenomen in artikel 127/4 van de WEC).
Le présent article est applicable lorsqu'un service de communications électroniques est fourni en Belgique.	Dit artikel is van toepassing wanneer elektronische-communicatiedienst in België wordt verstrekt.
L'ancien article 127, § 2, contenait une interdiction pour les opérateurs de rendre difficile ou impossible l'identification des utilisateurs finaux. Le nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés ou à tout le moins de rendre cette identification possible.	Het oude artikel 127, § 2, bevatte een verbod voor de operatoren om de identificatie van de eindgebruikers te bemoeilijken of onmogelijk te maken. Het nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren of op zijn minst deze identificatie mogelijk te maken.
Il n'est plus nécessaire de faire référence à la notion de fournisseur, étant donné que la notion d'opérateur est élargie dans le cadre de la transposition du Code des communications électroniques européen dans la loi télécom.	Het is niet langer noodzakelijk om te verwijzen naar het begrip van aanbieder aangezien het begrip van operator werd uitgebreid in het kader van de omzetting van het Europees wetboek voor elektronische communicatie in de telecomwet.
La notion d'abonné doit s'entendre au sens large et couvre également les personnes qui souscrivent aux services de l'opérateur à l'aide d'une carte prépayée ou qui souscrivent à un service d'un fournisseur au public de services de communications interpersonnelles non fondés sur la numérotation.	Het begrip van abonnee moet worden uitgebreid in de ruime zin en dekt ook de personen die intekenen op de diensten van de operator met behulp van een vooraf betaalde kaart of die intekenen op een dienst van een aanbieder aan het publiek van nummeronafhankelijke interpersoonlijke communicatiediensten.
Identifier un abonné qui est une personne physique signifie collecter et conserver ses données d'identification (ex. nom, prénom, date de naissance) et/ou une copie de son document d'identité (ex. passeport) et vérifier que cette identification est fiable (les documents/données sont fiables et correspondent à l'abonné). Il s'agit de la méthode d'identification directe de l'abonné. Un exemple d'une telle méthode est la lecture électronique de la carte d'identité belge, combinée avec l'utilisation de checkdoc.be,	Een abonnee identificeren die een natuurlijke persoon is, houdt in dat zijn identificatiegegevens (bijv. naam, voornaam, geboortedatum) en/of een kopie van zijn identiteitsstuk (bijv. paspoort) worden vergaard en bewaard en dat wordt nagegaan dat deze identificatie betrouwbaar is (de documenten/data zijn betrouwbaar en komen overeen met de abonnee). Het betreft de methode van directe identificatie van de abonnee. Een voorbeeld van een dergelijke methode is het elektronisch uitlezen van de

<p>qui est le site internet de vérification des documents d'identité belges.</p>	<p>Belgische identiteitskaart, in combinatie met het gebruik van checkdoc.be, de website voor verificatie van Belgische identiteitsstukken.</p>
<p>Rendre l'identification possible signifie qu'il doit être possible pour les autorités visées à l'article 127/1 qui sont habilitées par leur loi organique à obtenir de l'opérateur l'identité de l'abonné, sur la base des informations détenues par l'opérateur, de retrouver l'identité de l'abonné. Il s'agit de la méthode d'identification indirecte de l'abonné. A nouveau, il est essentiel que cette identification soit fiable. Un exemple d'identification indirecte est l'identification de l'abonné sur la base d'une opération de paiement électronique en ligne spécifique à l'achat ou la recharge d'une carte prépayée prévue à l'article 17 de 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.</p>	<p>De identificatie mogelijk maken houdt in dat de autoriteiten bedoeld in artikel 127/1 die krachtens hun organieke wet gemachtigd zijn om van de operator de identiteit van de abonnee te verkrijgen, in staat moeten zijn om op basis van de informatie in het bezit van de operator, de identiteit van de abonnee terug te vinden. Het betreft de methode van indirecte identificatie van de abonnee. Ook hierbij is het van essentieel belang dat deze identificatie betrouwbaar is. Een voorbeeld van indirecte identificatie is de identificatie van de abonnee op basis van een onlineverrichting van een elektronische betaling die specifiek bedoeld is om een vooraf betaalde kaart aan te kopen of te herladen, zoals vastgelegd in artikel 17 van het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een vooraf betaalde kaart.</p>
<p>L'identification indirecte présente l'avantage que l'opérateur ne connaît pas lui-même l'identité de son abonné lorsqu'il n'est pas nécessaire qu'il la connaisse. Cependant, cette identification indirecte rend également la tâche plus difficile pour les autorités. Il faut aussi rappeler que les opérateurs qui permettent l'accès aux services d'urgence qui offrent de l'aide sur place doivent pouvoir leur envoyer, lors de l'appel d'urgence, le nom et le prénom de l'appelant, en vertu de l'article 107, § 4, alinéa 1er, de la LCE.</p>	<p>De indirecte identificatie heeft als voordeel dat de operator zelf de identiteit van zijn abonnee niet kent wanneer het niet nodig is dat hij die kent. Toch bemoeilijkt deze indirecte identificatie de taak voor de autoriteiten. Er dient ook te worden aan herinnerd dat de operatoren die de toegang mogelijk maken tot de nooddiensten die ter plaatse hulp bieden, hen, in geval van een noodoproep, de naam en de voornaam van de beller moeten kunnen sturen, krachtens artikel 107, § 4, eerste lid, van WEC.</p>
<p>L'identification indirecte est introduite dans la législation étant donné qu'à la suite de la transposition du Code des communications électroniques européen, la notion d'opérateur sera étendue de manière à inclure également les fournisseurs au public de services de communications interpersonnelles non fondés sur la numérotation et que ces derniers disposent rarement de l'identité de leurs abonnés (identification directe). Vu l'utilisation croissante des services de ces fournisseurs, il n'est pas concevable qu'ils n'aient aucune obligation en matière</p>	<p>De indirecte identificatie wordt geïntroduceerd in de wetgeving aangezien naar aanleiding van de omzetting van het Europees Wetboek voor elektronische communicatie, het begrip van operator zal worden uitgebreid om ook de aanbieders aan het publiek van nummeronafhankelijke interpersoonlijke communicatiediensten te omhelzen en dat deze laatsten maar zelden over de identiteit van hun abonnees beschikken (directe identificatie). Gezien het toenemende gebruik van de diensten van deze aanbieders is het ondenkbaar dat hen geen enkele verplichting</p>

d'identification de leurs abonnés. Pour ces fournisseurs, une telle identification peut notamment être rendue possible par le biais de la conservation de l'adresse IP utilisée lors de la création du compte ou par le biais des informations relatives aux moyens de paiement utilisés. Cette méthode d'identification indirecte est également disponible pour les autres opérateurs que ces fournisseurs, sous réserve de restrictions qui seraient imposées par arrêté royal.	wordt opgelegd wat betreft de identificatie van hun abonnees. Voor deze aanbieders kan een dergelijke identificatie met name mogelijk gemaakt worden via de bewaring van het IP-adres gebruikt om de account te creëren of via informatie met betrekking tot de gebruikte betalingsmiddelen. Ook de andere operatoren buiten deze aanbieders kunnen deze methode van indirecte identificatie gebruiken, mits er beperkingen gelden die zouden worden opgelegd bij koninklijk besluit.
Il revient aux opérateurs de trouver les méthodes les plus appropriées pour identifier leurs abonnés ou pour rendre cette identification possible, en respectant la législation (notamment l'article 107, § 4, alinéa 1er, et la législation en matière de protection de la vie privée et des données à caractère personnel) et en tenant en compte des besoins des autorités.	Het is aan de operatoren om de meest geschikte manieren te vinden om hun abonnees te identificeren of deze identificatie mogelijk te maken, met inachtneming van de wetgeving (meer bepaald de artikelen 107, § 4, eerste lid, en de wetgeving inzake de bescherming van de persoonlijke levenssfeer en de persoonsgebonden gegevens) en rekening houdend met de noden van de autoriteiten.
L'obligation d'identification des abonnés s'applique lorsqu'un service de communications électroniques est offert en Belgique (même si l'opérateur n'y dispose pas d'un réseau).	De verplichting tot identificatie van de abonnees is van toepassing wanneer een elektronische-communicatiedienst wordt aangeboden in België (ook wanneer de operator er niet over een netwerk beschikt).
Il convient de noter que dans son arrêt Quadrature du Net du 6/10/2020 (aff. jointes C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.), la Cour de Justice de l'Union européenne a indiqué que la conservation des données relatives à l'identité civile constitue une ingérence non grave dans les droits repris dans la Charte des droits fondamentaux de l'Union européenne (en particulier le droit à la vie privée et le droit à la protection des données à caractère personnel).	Er dient te worden opgemerkt dat in zijn arrest-Quadrature du Net van 6/10/2020 (gevoegde zaken C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.), het Europees Hof van Justitie heeft aangegeven dat de bewaring van gegevens met betrekking tot de burgerlijke identiteit, een niet-ernstige inmenging vormt in de rechten vervat in het Handvest van de grondrechten van de Europese Unie (in het bijzonder het recht op de persoonlijke levenssfeer en het recht op de bescherming van de persoonsgebonden gegevens).
La disposition qui indique que l'opérateur est le responsable du traitement a été déplacée vers un article commun à plusieurs dispositions (voir art. 127/3).	De bepaling die aangeeft dat de operator verantwoordelijk is voor de verwerking, werd verplaatst naar een gemeenschappelijk artikel voor verscheidene bepalingen (zie art. 127/3).
C'est l'abonné (celui qui conclut le contrat avec l'opérateur) qui doit s'identifier auprès de l'opérateur.	Het is de abonnee (de persoon die het contract afsluit met de operator) die zich moet identificeren bij de operator.

<p>Afin de permettre à un opérateur d'identifier ses abonnés, l'article 127 vise dorénavant le recours au traitement automatisé de données biométriques. En pratique, l'opérateur peut comparer des photos que l'abonné prend lui-même de son visage avec la photo figurant sur son document d'identité. De la sorte, l'opérateur peut s'assurer que la personne qui entend s'identifier est bien la même personne que la personne dont la photo se trouve sur le document d'identité.</p>	<p>Opdat een operator zijn abonnees kan identificeren beoogt artikel 127 voortaan het gebruik van de geautomatiseerde verwerking van biometrische gegevens. In de praktijk kan de operator foto's die de abonnee zelf van zijn gezicht neemt vergelijken met de foto die op zijn identiteitsstuk staat. Op die manier kan de operator zich ervan vergewissen dat de persoon die zich wil identificeren wel degelijk dezelfde persoon is als diegene van wie de foto op het identiteitsstuk staat.</p>
<p>La modification législative est introduite pour tenir compte de l'article 6, § 4, de la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, tel que modifié par la loi du 25/11/2018. Il ressort de cet article que la photographie du titulaire ne peut être utilisée que si cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.</p>	<p>De wetswijziging wordt ingevoerd om rekening te houden met artikel 6, § 4, van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten, zoals gewijzigd bij de wet van 25/11/2018. Uit dat artikel blijkt dat de foto van de houder maar mag worden gebruikt als dat gebruik is toegestaan door of krachtens een wet, een decreet of een ordonnantie.</p>
<p>Cette méthode innovante permet à l'abonné de plus facilement s'identifier, vu qu'il ne doit plus se rendre dans un point de vente de l'opérateur en vue de son identification. Les avancées technologiques en la matière ont augmenté la fiabilité de cette méthode. La loi permet cependant au Roi de soumettre certaines méthodes d'identification de l'utilisateur final à une autorisation du ministre et du ministre de la Justice. Cette autorisation préalable a pour objectif de s'assurer de la fiabilité de la méthode.</p>	<p>Met deze innoverende methode kan de abonnee zich makkelijker identificeren, aangezien hij niet meer naar een verkooppunt van de operator hoeft te gaan om zich te identificeren. De technologische vooruitgang op dat gebied heeft de betrouwbaarheid van die methode vergroot. De wet biedt de Koning evenwel de mogelijkheid om bepaalde methodes ter identificatie van de eindgebruiker te onderwerpen aan een machtiging van de minister en van de minister van Justitie. Deze voorafgaande machtiging heeft tot doel zich te vergewissen van de betrouwbaarheid van de methode.</p>
<p>Par ailleurs, le traitement de données biométriques bénéficie d'un haut niveau de protection à l'article 9 du RGPD, qui s'applique en l'espèce. En effet, en vertu de cet article, l'abonné de l'opérateur devra donner son consentement explicite au traitement de ses données. Pour que ce consentement soit libre, l'abonné doit avoir la possibilité de s'identifier autrement que via un traitement automatisé de ses données biométriques. De plus, en vertu du principe de minimisation des données visé à l'article 5 du RGPD, le traitement des données devra être</p>	<p>Bovendien wordt de verwerking van biometrische gegevens sterk beveiligd door artikel 9 van de AVG, die hier van toepassing is. Krachtens dat artikel moet de abonnee van de operator immers zijn uitdrukkelijke toestemming geven voor de verwerking van zijn gegevens. Om te kunnen spreken van een vrije toestemming moet de abonnee de mogelijkheid hebben om zich op een andere manier te identificeren dan via een geautomatiseerde verwerking van zijn biometrische gegevens. Krachtens het principe van de minimale</p>

limité à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, à savoir dans ce cas-ci s'assurer que la personne qui prend la photo correspond à la personne sur le document d'identité.	gegevensverwerking waarvan sprake in artikel 5 van de AVG, moet de gegevensverwerking beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt; in dit geval betekent dat: zich ervan vergewissen dat de persoon die de foto neemt overeenstemt met de persoon op het identiteitsstuk.
Si nécessaire, le Roi peut préciser, le cas échéant selon le type d'opérateurs et le type d'activités, la manière dont les utilisateurs finaux (en pratique les abonnés et les utilisateurs effectifs du service) doivent être identifiés, le cas échéant en imposant des obligations à ces derniers. A ce jour, cette délégation au Roi a été exécutée par 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, qui impose des obligations aux opérateurs et aux utilisateurs finaux.	Indien nodig kan de Koning desgevallend afhankelijk van het type van operatoren en het type van activiteiten de manier specificeren waarop de eindgebruikers (in de praktijk de abonnees en de daadwerkelijke gebruikers van de dienst) moeten geïdentificeerd worden, desgevallend door verplichtingen op te leggen aan deze laatste. Tot op heden werd deze machtiging van de Koning ten uitvoer gebracht krachtens het koninklijk besluit november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, dat verplichtingen oplegt aan de operatoren en aan de eindgebruikers.
Le paragraphe 3 de l'article 127 a été supprimé, étant donné la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité a mis fin à l'anonymat pour les cartes prépayées.	Paragraaf 3 van artikel 127 werd geschrapt aangezien de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst een einde heeft gemaakt aan de anonimiteit van de vooraf betaalde kaarten.
Art. 10	Art. 10
L'article 127/1 est une disposition commune aux articles 122, 123, 126, 126/1 et 127, qui comprend la liste des catégories d'autorités pouvant demander accès aux données d'identification de trafic et de localisation conservées auprès des opérateurs en vertu de ces articles au bénéfice des autorités, des utilisateurs finaux ou pour leurs propres besoins.	Artikel 127/1 is een gemeenschappelijke bepaling voor de artikelen 122, 123, 126, 126/1 en 127, die de lijst bevat van de categorieën van autoriteiten die toegang kunnen vragen tot de identificatie-, verkeers- en locatiegegevens, bewaard bij de operatoren krachtens deze artikelen ten behoeve van de autoriteiten, de eindgebruikers of voor hun eigen behoeften..

<p>Il convient de prendre en compte la jurisprudence concernant l'accès des autorités aux données conservées pour ces dernières :</p>	<p>Er dient rekening te worden gehouden met de jurisprudentie inzake inzage van de autoriteiten in de gegevens die voor deze laatste worden bewaard:</p>
<p>- arrêt <i>Quadrature du Net</i> du 6/10/2020 de la CJUE (C 511/18, 512/18 et 520/18) : «166 l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale. 167 À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58. » ;</p>	<p>- arrest <i>Quadrature du Net</i> van 6/10/2020 van het HvJ-EU (C 511/18, 512/18 en 520/18): "166 de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecomunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, [kan] in beginsel enkel [...] worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist [sic] de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen." 167 In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58. ";</p>

<ul style="list-style-type: none"> - pour ce qui concerne les adresses IP et la criminalité, la sécurité publique et la sécurité nationale, il ressort du même arrêt que seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale sont de nature à justifier la conservation de cette donnée (point 156) ; - dans son arrêt Prokuratuur du 2 mars 2021 (C-746/18), la CJUE a jugé que « L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) [...] doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période. » ; 	<ul style="list-style-type: none"> - wat betreft de IP-adressen en de criminaliteit, de openbare veiligheid en de nationale veiligheid, blijkt uit hetzelfde arrest dat enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, de bewaring van dit gegeven kunnen rechtvaardigen (punt 156); - in zijn arrest Prokuratuur van 2 maart 2021 (C-746/18) heeft het HvJ-EU geoordeeld: "Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) [...] moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer - welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid -, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn.";
--	--

<p>- dans son arrêt du 21/04/2021 (nos 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), le Conseil d'Etat français a indiqué que « <i>la conservation rapide des données susceptibles de contribuer à la recherche, la constatation et la poursuite des infractions pénales, dans le respect du principe de proportionnalité prévu par le code de procédure pénale conformément à ce qui a été rappelé au point 39, est possible dans les conditions prévues par la directive du 12 juillet 2002 et le RGPD, y compris, comme l'a jugé la Cour ainsi qu'il a été rappelé au point 55, lorsque cette conservation rapide porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. L'autorité judiciaire est donc en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie. Le même principe s'applique nécessairement aux autorités administratives indépendantes disposant d'un droit d'accès aux données de connexion en vertu de la loi en vue de lutter contre les manquements graves aux règles dont elles ont la charge d'assurer le respect.</i> » (point 57).</p>	<p>- in zijn arrest van 21/04/2021 (nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres) heeft de Franse Raad van State gesteld: "<i>de snelle bewaring van de gegevens die kunnen bijdragen tot het opsporen, vaststellen en vervolgen van strafbare feiten, met inachtneming van het proportionaliteitsbeginsel vastgesteld in het wetboek van strafvordering, overeenkomstig hetgeen is herhaald in punt 39, is mogelijk onder de voorwaarden waarin voorzien wordt door de richtlijn van 12 juli 2002 en de AVG, inclusief, zoals geoordeeld door het Hof, alsook herhaald in punt 55, wanneer die snelle bewaring betrekking heeft op gegevens die aanvankelijk waren bewaard ten behoeve van de nationale veiligheid. De gerechtelijke autoriteit kan dus inzage krijgen in de gegevens die nodig zijn voor het vervolgen en opsporen van de daders van strafbare feiten waarvan de ernst dit rechtvaardigt. Hetzelfde principe geldt noodzakelijkerwijs voor de onafhankelijke administratieve overheden die krachtens de wet over een inzagerecht in de connectiegegevens beschikken met het oog op de strijd tegen ernstige inbreuken op de regels die ze tot taak hebben te doen naleven.</i> » (punt 57) (vrij vertaald).</p>
<p>Les autorités peuvent obtenir accès aux données conservées en vertu des articles 122 et 123 pour les finalités visées à l'article 127/1.</p>	<p>De autoriteiten kunnen toegang tot de krachtens de artikelen 122 en 123 bewaarde gegevens krijgen voor de in artikel 127/1, genoemde doeleinden.</p>
<p>Les autorités peuvent obtenir accès aux données conservées en vertu des articles 126 et 127 pour les finalités pour lesquelles elles sont conservées, à savoir les finalités prévues à l'article 127/1.</p>	<p>Autoriteiten kunnen toegang tot de krachtens de artikelen 126 en 127 bewaarde gegevens krijgen voor de doeleinden waarvoor zij worden bewaard, namelijk de in artikel 127/1, genoemde doeleinden.</p>

<p>Les autorités peuvent obtenir accès aux données conservées en vertu de l'article 126/1 pour les finalités pour lesquelles elles sont conservées, à savoir aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique.</p> <p>La conservation ciblée sur base géographique peut également être utilisée dans le cadre de la sauvegarde des intérêts vitaux d'une personne physique. En pratique, on peut penser aux hypothèses suivantes : l'utilisation de données de localisation par la cellule personne disparue de la police fédérale (en cas de disparition inquiétante, la police ne peut pas toujours immédiatement déterminer s'il s'agit d'un acte criminel ou non) et par les services d'urgence offrant de l'aide sur place (100, 101 et 112). Pour ces derniers services, l'article 107 de la loi télécom prévoit que l'opérateur doit fournir les données de localisation de l'appelant aux services d'urgence qui offrent de l'aide sur place lors de l'appel. En cas de difficultés techniques pour la fourniture de ces données de localisation en temps réel, ces services doivent pouvoir obtenir les dernières données conservées de localisation de l'appelant.</p>	<p>Autoriteiten kunnen toegang tot de krachtens artikel 126/1, bewaarde gegevens krijgen voor de doeleinden waarvoor zij worden bewaard, namelijk ter vrijwaring van de nationale veiligheid, ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid en ter bescherming van de vitale belangen van een natuurlijke persoon.</p> <p>De gerichte bewaring op geografische basis kan ook worden toegepast in het kader van de vrijwaring van de vitale belangen van een natuurlijke persoon. In de praktijk kan men denken aan de volgende gevallen: het gebruik van locatiegegevens door de cel Vermiste Personen van de federale politie (in geval van een onrustwekkende verdwijning kan de politie niet altijd onmiddellijk bepalen of het om een misdrijf gaat of niet) en door de nooddiensten die ter plaatse hulp bieden (100, 101 en 112). Voor die laatste diensten schrijft artikel 107 van de telecomwet voor dat de operator tijdens de oproep de locatiegegevens van de oproeper moet verstrekken aan de nooddiensten die ter plaatse hulp bieden. Bij technische moeilijkheden voor de realtime-verstrekking van deze locatiegegevens moeten deze diensten de laatste, bewaarde locatiegegevens van de oproeper kunnen krijgen.</p>
<p>Dans le cadre de leurs compétences, les autorités obtiennent accès aux données conservées par les opérateurs au bénéfice des autorités, des utilisateurs finaux ou pour leurs propres besoins pour autant que cela soit prévu par leur loi organique et dans les conditions de cette dernière.</p>	<p>In het kader van hun bevoegdheden verkrijgen de autoriteiten toegang tot de gegevens die door de operatoren worden bewaard ten behoeve van de autoriteiten, de eindgebruikers of voor hun eigen behoeften, voor zover dat is bepaald in hun organieke wet en in de voorwaarden van die wet.</p>
<p>L'article 127/1 ne s'applique pas lorsqu'une partie à la communication transmet des données à une autorité.</p>	<p>Artikel 127/1 is niet van toepassing wanneer een bij de communicatie betrokken partij gegevens doorstuurt naar een autoriteit.</p>
<p>Les objectifs de cette liste sont, d'une part, d'apporter, dans une certaine mesure, de la sécurité juridique aux opérateurs quant aux autorités disposant d'un droit d'accès aux données qu'ils conservent, et, d'autre part, d'apporter de la transparence aux utilisateurs finaux quant à l'utilisation de leurs données d'identification, de trafic et de localisation.</p>	<p>De doelstellingen van deze lijst zijn enerzijds om, in een zekere mate, de operatoren rechtszekerheid te bieden wat betreft de autoriteiten die het recht hebben om toegang te krijgen tot de gegevens die ze bewaren en anderzijds om de eindgebruikers transparantie te geven over het gebruik van</p>

	hun identificatie-, verkeers- en locatiegegevens.
Avant de donner suite à une demande d'une autorité d'obtenir des données de l'opérateur, il est attendu de ce dernier de s'assurer que cette autorité dispose bien d'une base légale pour requérir les données. Mais il ne revient pas à l'opérateur de juger de la proportionnalité des demandes d'accès de cette autorité.	Alvorens gevolg te geven aan een verzoek van een autoriteit om gegevens te krijgen van de operator, wordt van deze laatste verwacht dat hij zich ervan vergewist dat die autoriteit wel degelijk bij wet bevoegd is om de gegevens op te vragen. Maar het is niet aan de operator om te oordelen over de evenredigheid van de verzoeken om inzage van die autoriteit.
Le présent article reprend une liste de finalités et non plus une liste d'autorités comme c'était le cas de l'ancienne liste de l'article 126, § 2 et ce pour les raisons suivantes.	Dit artikel bevat een lijst van doeleinden en niet langer een lijst van autoriteiten zoals dat het geval was voor de oude lijst van artikel 126, § 2, om de volgende redenen.
Cela permet d'assurer que la législation couvre les différents cas de figure et les évolutions futures. A cet égard, il convient de noter qu'il est rapidement apparu que la liste fermée des autorités visées à l'article 126, § 2 était incomplète. L'adaptation de cette liste fermée s'est révélée être un exercice difficile (par exemple car la loi est attaquée devant la Cour constitutionnelle et peut difficilement être modifiée) et très lent, alors que le fait pour une autorité de ne pas figurer sur la liste, alors que c'est nécessaire, provoque immédiatement des difficultés opérationnelles pour cette dernière.	Zo kan ervoor gezorgd worden dat de wetgeving de verschillende gevallen en de toekomstige ontwikkelingen beslaat. In dat kader dient te worden opgemerkt dat al snel is gebleken dat de besloten lijst van autoriteiten bedoeld in artikel 126, § 2, onvolledig was. De aanpassing van deze lijst is een moeilijke oefening (bijvoorbeeld omdat de wet werd aangevochten bij het Grondwettelijk Hof en maar moeilijk kan gewijzigd worden) en erg trage oefening gebleken, terwijl een overheid onmiddellijk operationele problemen ondervindt wanneer ze niet op de lijst staat, terwijl dat wel nodig is.
Les données d'identification et de souscription visées par les articles 126 et 127 sont des données basiques dont ont besoin un nombre non négligeable d'autorités. On peut s'attendre à ce que ce nombre augmente à l'avenir, étant donné la croissance du nombre d'infractions en ligne. Il est également très difficile de faire une liste exhaustive de toutes les dispositions légales qui permettent aux différentes autorités d'obtenir des opérateurs des données d'identification, de trafic ou de localisation.	De identificatie- en abonnementsgegevens bedoeld in de artikelen 126 en 127 zijn basisgegevens die benodigd zijn door een niet-verwaarloosbaar aantal autoriteiten. Dat aantal zal wellicht toenemen in de toekomst gezien de groei van het aantal online-inbreuken. Het is ook erg moeilijk om een volledige lijst op te stellen, met alle wettelijke bepalingen die de verschillende autoriteiten in staat stellen om de identificatie-, verkeers- en locatiegegevens te verkrijgen van de operatoren.
Pour qu'une autorité puisse obtenir des données de l'opérateur, il est nécessaire qu'elle réponde à une des finalités visées à l'article 127/1 et que sa loi organique ou sectorielle lui donne le pouvoir d'obtenir ces données de l'opérateur.	Opdat een autoriteit gegevens kan krijgen van de operator, is het nodig dat ze beantwoordt aan een van de doeleinden bedoeld in artikel 127/1 en dat haar organieke of sectorale wet haar machtigt om deze gegevens te krijgen van de operator.

Ce sont ces lois organiques ou sectorielles qui doivent fixer les conditions d'accès des autorités aux données.	Het zijn die organieke of sectorale wetten die de voorwaarden voor toegang tot de gegevens door de autoriteiten moeten vastleggen.
Les données doivent être obtenues par le biais de la Cellule de coordination de l'opérateur. Cela n'empêche évidemment que la réponse de cette cellule soit envoyée de manière automatique (sans intervention humaine).	De gegevens moeten worden verkregen via de Coördinatiecel van de operator. Dat neemt natuurlijk niet weg dat het antwoord van die cel automatisch wordt verstuurd (zonder menselijke tussenkomst).
Les infractions pénales doivent être entendues au sens large du terme, en ce compris couvrant les fraudes qui constituent des infractions pénales.	De strafrechtelijke inbreuken moeten worden uitgebreid in de brede zin van de term, inclusief gevallen van fraude die strafbare feiten vormen.
De même, la nature pénale d'une sanction administrative s'apprécie au regard de la jurisprudence de la Cour européenne des droits de l'homme.	Zo ook dient de strafrechtelijke aard van een administratieve sanctie te worden gezien in het licht van de rechtspraak van het Europees Hof voor de Rechten van de Mens.
La « matière pénale » au sens de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales se fonde sur trois critères : « Le premier est la qualification juridique de l'infraction en droit interne, le second la nature même de l'infraction et le troisième le degré de sévérité de la sanction que risque de subir l'intéressé. Les deuxième et troisième critères sont alternatifs et pas nécessairement cumulatifs. Cela n'empêche pas l'adoption d'une approche cumulative si l'analyse séparée de chaque critère ne permet pas d'aboutir à une conclusion claire quant à l'existence d'une accusation en matière pénale » (Cour eur. D.H., arrêt Sergueï Zolotoukhine c. la Russie (GC), du 10 février 2009, n° 53).	De strafrechtelijke materie in de zin van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden is gebaseerd op drie criteria: Het eerste is de juridische kwalificatie van de inbreuk in intern recht, het tweede de eigenlijke aard van de inbreuk en het derde de zwaarte van de straf die de betrokkene riskeert te ondergaan. Het tweede en het derde criterium zijn alternatief en niet noodzakelijk cumulatief. Dit belet niet dat een cumulatieve benadering aangenomen wordt indien aan de hand van de afzonderlijke analyse van elk criterium geen duidelijke conclusie mogelijk is over het bestaan van een strafrechtelijke beschuldiging" (EHRM, arrest Sergey Zolotukhin/Rusland (GC) van 10 februari 2009, nr. 53) (vrij vertaald).
À titre d'exemple d'une telle sanction administrative à caractère pénal, l'on peut donner l'amende administrative que peut imposer la FSMA, entre autres en cas d'infraction à l'interdiction d'abus de marché. La nature pénale de ces sanctions est principalement due au fait que la jurisprudence européenne établit que ces sanctions administratives sont également de nature punitive et que ces procédures administratives doivent être accompagnées de toutes les garanties en matière de droits de la défense (art. 6 de la CEDH). Il en va donc	Als voorbeeld van dergelijke administratieve sanctie met strafkarakter kan de administratieve geldboete gegeven worden die de FSMA kan opleggen, onder meer bij een inbreuk op het verbod op marktmisbruik. Onder meer uit de rechtspraak van het Europees Hof voor de rechten van de mens kan worden afgeleid dat deze administratieve geldboete een strafkarakter heeft, omdat de bepalingen waarvan de schending wordt verweten tot doel hebben het algemeen belang van de samenleving te vrijwaren, dat normaal beschermd wordt door het strafrecht,

de même pour le principe ne bis in idem. Lorsqu'on impose une telle sanction administrative, il faut dès lors également prendre en compte les éventuelles sanctions pénales, ou vice versa.	en omdat omwille van het maximum dat zij theoretisch kan bereiken, de sanctie zowel een ontradend als een punitief karakter heeft (zie onder meer overwegingen 94 en volgende van het arrest Grande Stevens van het EHRM van 4 maart 2014, nr. 18640/10, en de daar geciteerde referenties).
Les autorités visées au premier point (1°) comprennent, outre les autorités judiciaires et les officiers de police judiciaire, par exemple les autorités suivantes :	Tot de autoriteiten bedoeld in het eerste punt (1°) behoren, naast de gerechtelijke autoriteiten en de officieren van gerechtelijke politie, bijvoorbeeld de volgende autoriteiten:
<ul style="list-style-type: none"> - l'auditeur de la FSMA qui, dans le cadre de son instruction sur d'éventuelles infractions à la législation financière relevant du domaine de compétences de la FSMA, notamment dans le cadre d'une instruction sur un éventuel abus de marché, a le pouvoir de requérir de telles données ; 	<ul style="list-style-type: none"> - de auditeur van de FSMA, die in het kader van zijn onderzoek naar inbreuken op de financiële wetgeving die onder de bevoegdheid van de FSMA ressorteert, zo o.m. in het kader van een onderzoek naar marktmisbruik, de bevoegdheid heeft om dergelijke gegevens op te vragen;
<ul style="list-style-type: none"> - l'auditeur de l'Autorité belge de la concurrence qui, dans le cadre de son instruction sur d'éventuelles infractions aux règles du droit de la concurrence, a le pouvoir de requérir des données ; 	<ul style="list-style-type: none"> - de auditeur van de Belgische Mededingingsautoriteit die, in het kader van zijn onderzoek naar eventuele inbreuken op de regels van het mededingingsrecht, bevoegd is om gegevens op te vragen;
<ul style="list-style-type: none"> - le CCB car ses différentes tâches légales, telles que fixées par l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique et 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 (loi NIS), visent notamment à prévenir et détecter les infractions pénales en matière de cybercriminalité (diffusion de messages d'alerte ou d'informations sur les risques et incidents auprès des parties intéressées ; information et sensibilisation des utilisateurs des systèmes d'information et de communication) ; 	<ul style="list-style-type: none"> - het CCB want zijn verschillende wettelijke taken, zoals bepaald bij het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België en 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 (NIS-wet), zijn er meer bepaald op gericht om de strafbare feiten inzake cybercriminaliteit te voorkomen en op te sporen (verspreiden van waarschuwingen of informatie over de risico's en incidenten onder de geïnteresseerden; informeren en sensibiliseren van de gebruikers van informatie- en communicatiesystemen);
<ul style="list-style-type: none"> - les agents visés à l'article XV.2, § 1er du Code de droit économique, en vue de l'exercice de la compétence visée à l'article XV.3, 5°/1 du même Code, 	<ul style="list-style-type: none"> - de ambtenaren bedoeld in artikel XV.2, § 1 van het Wetboek van economisch recht, met het oog op de uitoefening van de bevoegdheid als

<p>dans le cadre de leurs compétences légalement attribuées. Ces agents peuvent demander aux opérateurs les données permettant l'identification des auteurs d'infractions aux législations qui relèvent de leurs compétences, agissant sous l'anonymat, sous une fausse dénomination, sous un pseudonyme ou toute autre forme qui empêche de connaître l'identité réelle de l'acteur économique.</p>	<p>bedoeld in artikel XV.3, 5°/1 van hetzelfde Wetboek, in het kader van hun wettelijk toegekende bevoegdheden. Deze ambtenaren mogen aan de operatoren de gegevens vragen die de identificatie mogelijk maken van plegers van de inbreuken op de wetgevingen die onder hun bevoegdheid vallen, die anoniem handelen, onder een valse benaming, onder een pseudoniem of onder een andere vorm die verhindert de werkelijke identiteit van de economische speler te kennen.</p>
<p>Le service de médiation pour les télécommunications est une autorité chargée d'apporter de l'aide aux personnes, étant donné qu'il fournit à la victime d'une utilisation malveillante du réseau (en particulier le harcèlement téléphonique), le nom, le prénom et l'adresse de l'auteur de cette utilisation conformément à l'article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.</p>	<p>De Ombudsdienst voor telecommunicatie is een autoriteit die is belast met het bieden van hulp aan personen aangezien hij aan slachtoffers van kwaadwillig gebruik van het netwerk (in het bijzonder van telefonische pesterijen) de naam, voornaam en het adres van de dader van dat gedrag verstrekt conform artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven.</p>
<p>Les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service sont notamment l'IBPT et le Centre pour la Cybersécurité Belgique (CCB). En sa qualité de CSIRT national, le CCB est, en effet, chargé, en vertu de l'article 60 de la loi NIS (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) de la détection, de l'observation et de l'analyse des problèmes de sécurité informatique en Belgique.</p>	<p>De autoriteiten bevoegd voor het onderzoek van een veiligheidsprobleem op het netwerk of van de dienst zijn met name het BIPT en het Centrum voor Cybersecurity België (CCB). In zijn hoedanigheid van nationaal CSIRT is het CCB immers, krachtens artikel 60 van de NIS-wet (wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid), belast met het opsporen, observeren en analyseren van computerbeveiligingsproblemen in België.</p>
<p>Pour accroître la transparence envers le citoyen, l'IBPT publiera sur son site Internet des informations sur l'accès des autorités aux données d'identification, de trafic et de localisation. Il reviendra aux autorités concernées de fournir à l'IBPT les informations que ce dernier publiera sur son site internet.</p>	<p>Om de transparantie ten aanzien van de burger te vergroten, zal het BIPT op zijn website informatie publiceren over de toegang van de autoriteiten tot de identificatie-, verkeers- en locatiegegevens. Het zal aan de betrokken autoriteiten zijn om aan het BIPT de informatie te verstrekken die deze laatste zal publiceren op zijn website.</p>
<p>Art. 11</p>	<p>Art. 11</p>

La communication des statistiques est généralisée à l'accès des autorités à l'ensemble des données conservées en vertu des articles 122, 123, 126, 126/1 et 127.	De mededeling van de statistieken wordt veralgemeend met de toegang van de autoriteiten tot het geheel van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127.
Il est ajouté une obligation complémentaire à charge des opérateurs : celle de garantir la qualité des données conservées en vertu des articles 122, 123, 126, 126/1 et 127. Dès lors que ces données peuvent, sous certaines conditions, être utilisées notamment à des fins de sauvegarde de la sécurité nationale et de lutte contre la criminalité, il est crucial que leur qualité soit incontestable. Dans cet objectif, les opérateurs prennent toutes les mesures adéquates pour garantir en tout temps leur exactitude, leur intégrité et leur fiabilité.	Er wordt een bijkomende verplichting toegevoegd voor de operatoren: deze om de kwaliteit van de gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127, te garanderen. Aangezien deze gegevens, onder bepaalde voorwaarden, kunnen worden gebruikt met name voor doeleinden van vrijwaring van de nationale veiligheid en strijd tegen de criminaliteit, is het onontbeerlijk dat ze van onomstotelijke kwaliteit zijn. Daartoe treffen de operatoren alle gepaste maatregelen om te allen tijde de juistheid, integriteit en betrouwbaarheid ervan te garanderen.
Il revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre, les opérateurs doivent être mesure d'établir des liens entre les données conservées pour les autorités. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur base de différents articles.	Het is aan de operatoren om te beslissen hoe ze zich organiseren voor de bewaring van de gegevens ten behoeve van de autoriteiten (in het bijzonder de gegevens bewaard conform de artikelen 126, 126/1, 127). Wanneer eenzelfde gegeven wordt bedoeld in verscheidene artikelen, mogen ze dat gegeven dus één keer bewaren. De operatoren moeten daarentegen in staat zijn om verbanden te leggen tussen de gegevens bewaard voor de autoriteiten. Dat is nodig aangezien een operator, om te antwoorden op een verzoek van een autoriteit, genoopt zou kunnen zijn om gegevens te raadplegen die zijn bewaard op basis van verschillende artikelen.
Le paragraphe 3, alinéa 1er, reprend des mesures de protection des données conservées par les opérateurs pour les autorités.	Paragraaf 3, eerste lid, vermeldt maatregelen ter bescherming van de door de operatoren voor de autoriteiten bewaarde gegevens.
Un opérateur ne peut pas utiliser pour ses propres besoins les données qu'ils conservent pour les autorités. Bien entendu, un opérateur peut conserver une même donnée pour plusieurs finalités (pour ses propres besoins et pour les autorités).	Een operator mag de gegevens die hij bewaart voor de autoriteiten, niet voor zijn eigen behoeften gebruiken. Een operator kan eenzelfde gegeven uiteraard voor verscheidene doeleinden bewaren (voor zijn eigen behoeften en voor de autoriteiten).
Le paragraphe 3, alinéa 2, reprend des mesures de protection des données conservées par les opérateurs et auxquelles les autorités pourraient demander accès.	Paragraaf 3, tweede lid, vermeldt maatregelen ter bescherming van de door de operatoren bewaarde gegevens waartoe de autoriteiten toegang zouden kunnen vragen.

Lorsque le délai de conservation d'une donnée est atteint, l'opérateur supprime la donnée ou la rend anonyme. Ce principe est mis en œuvre dans les articles 122 et 123 de la loi. Bien entendu, l'opérateur ne pourra pas supprimer la donnée ou la rendre anonyme s'il a reçu une injonction d'une autorité de prolonger la durée de conservation de la donnée (conservation rapide des données ou « quick freeze »).	Wanneer de bewaringstermijn van een gegeven bereikt is, verwijdt de operator het gegeven of maakt hij het anoniem. Dat principe wordt ten uitvoer gebracht in de artikelen 122 en 123 van de wet. De operator zal het gegeven natuurlijk niet mogen schrappen of anoniem maken wanneer hij een bevel heeft gekregen van een overheid om de bewaringstermijn van het gegeven te verlengen (snelle bewaring van de gegevens of "quick freeze").
La demande à la Cellule de coordination ainsi que la réponse de cette dernière peuvent avoir lieu de manière automatisée.	Het verzoek aan de Coördinatiecel alsook het antwoord van deze laatste, kan automatisch verlopen.
Ce journal porte sur les demandes des différentes autorités en matière de données d'identification, de trafic ou de localisation.	Dit logboek heeft betrekking op de aanvragen van de verschillende autoriteiten inzake de identificatie-, verkeers- en locatiegegevens.
L'obligation d'enregistrement (« log ») automatisé dans le journal de chaque accès aux données conservées par l'opérateur pour les autorités a pour objectif d'éviter qu'il ne soit possible d'accéder à ces données sans trace de cet accès dans le journal. De la sorte, un accès non autorisé (abus) aux données pourra être retrouvé grâce au journal.	De verplichting tot automatische registratie ("log") in het logboek van elke toegang tot de gegevens die de operator bewaart voor de autoriteiten, heeft tot doel te vermijden dat toegang tot die gegevens mogelijk is zonder sporen ervan in het logboek. Zo kan een niet-toegestane toegang (misbruik) tot de gegevens teruggevonden worden dankzij het logboek.
Une distinction est faite entre l'accès aux données conservées par l'opérateur aux fins des autorités et l'accès aux données qu'il conserve pour ses propres fins, car pour ce qui concerne la deuxième catégorie, différentes équipes de l'opérateur (par exemple son équipe facturation ou anti-fraude), et pas uniquement sa cellule de coordination, doivent pouvoir accéder à ces données. Pour assurer des règles proportionnées, l'obligation d'enregistrement de l'accès aux données conservées par l'opérateur pour ses propres fins ne vaut que pour sa cellule de coordination.	Er wordt een onderscheid gemaakt tussen de toegang tot de gegevens die de operator bewaart voor doeleinden van de autoriteiten en de toegang tot de gegevens die hij bewaart voor zijn eigen doeleinden, want wat die tweede categorie betreft, moeten verschillende teams van de operator (bijvoorbeeld zijn factureringsteam of zijn antifraudeteam) en niet enkel zijn Coördinatiecel, toegang kunnen hebben tot die gegevens. Om te zorgen voor evenredige regels, geldt de verplichting tot registratie van de toegang tot de gegevens die de operator bewaart voor zijn eigen doeleinden enkel voor zijn Coördinatiecel.
L'objectif du journal est de permettre de vérifier si l'accès à une donnée conservée était bien justifié par une demande d'une autorité et, si ce n'est pas le cas, de retrouver la personne qui a accédé aux données.	Het doel van het logboek bestaat erin om na te gaan of de toegang tot een bewaard gegeven wel degelijk gerechtvaardigd is door een verzoek van een overheid en, indien dat niet het geval is, om de persoon die toegang heeft gehad tot de gegevens, terug te vinden.

Le journal doit permettre de prendre facilement connaissance de la demande de l'autorité (ou d'une copie de cette demande). Seul ce qui est demandé à l'opérateur doit être repris dans le journal.	Via het logboek moet gemakkelijk kennis kunnen worden genomen van het verzoek van de autoriteit (of van een kopie van dat verzoek). Enkel wat wordt gevraagd aan de operator moet worden opgenomen in het logboek.
L'opérateur ne doit pas conserver dans le journal la réponse envoyée à l'autorité mais bien les « métadonnées » liées à cette réponse. En cas de doute sur la légalité d'un accès aux données conservées, cela permettra de rechercher la réponse envoyée à l'autorité et, le cas échéant, de contacter l'autorité indiquée dans le journal.	De operator hoeft het aan de autoriteit gestuurde antwoord niet te bewaren in het logboek maar wel de "metagegevens" in verband met dat antwoord. In geval van twijfel over de wettelijkheid van een toegang tot de bewaarde gegevens, kan op die manier het antwoord dat werd verstuurd aan de autoriteit worden opgezocht en desgevallend contact worden opgenomen met de autoriteit vermeld in het logboek.
Lorsqu'une autorité formule sa demande dans un document et reprend en annexe de ce document les finalités et le contexte de l'enquête ou des informations qui justifient la demande, l'opérateur devra conserver dans le journal (une copie de) ce document (la demande) mais ne pourra pas y conserver les annexes.	Wanneer een autoriteit haar verzoek in een document formuleert en als bijlage bij dat document de doeleinden en de context van het onderzoek of informatie ter rechtvaardiging van het verzoek opneemt, dan moet de operator in het logboek (een kopie van) dat document (het verzoek) bewaren maar zonder de bijlagen erbij.
Par contre, si ces finalités, ce contexte ou ces informations sont incorporés dans la demande de l'autorité (et n'en sont pas dissociables), l'opérateur devra enregistrer dans le journal la copie de la demande sans la modifier.	Indien die doeleinden, die context of die informatie daarentegen zijn opgenomen in het verzoek van de autoriteit (en daar niet van kunnen worden losgekoppeld), dan zal de operator in het logboek de kopie van het verzoek moeten opnemen zonder het te wijzigen.
La tenue du journal, l'accès à celui-ci et les modifications qui y sont apportées doivent faire l'objet d'une procédure claire et conforme aux standards du RGPD, de manière à garantir l'authenticité et l'intégrité des données. Il est essentiel qu'il ne soit pas possible de manipuler de manière non autorisée le journal, ce qui lui ferait perdre toute sa valeur.	Het houden van het logboek, de toegang ertoe en de wijzigingen die erin worden aangebracht, moeten het voorwerp uitmaken van een duidelijke procedure die in overeenstemming is met de standaarden van de AVG, zodat de authenticiteit en de integriteit van de gegevens gewaarborgd zijn. Het is van essentieel belang dat het niet mogelijk is om op niet-toegestane wijze handelingen uit te voeren in verband met het logboek, wat het zou ontdoen van alle waarde.
Dans le cadre du contrôle de l'opérateur, l'IBPT et l'Autorité de protection des données peuvent consulter le journal ou exiger une copie de ce dernier. Cela n'empêche pas une consultation du journal dans un autre cadre (par exemple par le juge d'instruction si une	In het kader van de controle van de operator kunnen het BIPT en de Gegevensbeschermingsautoriteit het logboek raadplegen of een kopie ervan eisen. Dat neemt niet weg dat het logboek in een ander kader kan worden geraadpleegd (bijvoorbeeld

personne a accédé aux données de manière illégale).	door de onderzoeksrechter indien een persoon toegang heeft gehad tot de gegevens op een onwettige manier).
La disposition ne reprend pas l'obligation pour l'IBPT et l'Autorité de protection des données de conclure un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal, étant donné que ce protocole n'a pas été établi à ce jour. Cela n'empêche pas qu'il soit tout de même conclu, si cela s'avérait nécessaire.	De bepaling neemt de verplichting voor het BIPT en de Gegevensbeschermingsautoriteit niet over om een samenwerkingsprotocol te sluiten over het kennisnemen en controleren van de inhoud van het logboek, aangezien dat protocol tot op heden niet is opgesteld. Dat belet niet dat het toch gesloten wordt, indien dat nodig zou blijken.
La possibilité de demander un audit externe a été ajoutée de manière à faciliter le contrôle par l'IBPT du respect des obligations à charge des opérateurs. L'opérateur pourra proposer à l'IBPT un organisme et il reviendra à l'IBPT de marquer son accord avant que cet organisme puisse effectuer le contrôle. Dans le cadre de son accord, l'IBPT examinera si l'organisme est bien qualifié et indépendant.	De mogelijkheid om een externe audit te vragen werd toegevoegd teneinde de controle door het BIPT op de inachtneming van de verplichtingen ten laste van de operatoren te vergemakkelijken. De operator zal aan het BIPT een instantie kunnen voorstellen en het zal aan het BIPT zijn om zijn akkoord te geven alvorens die instantie de controle mag uitvoeren. In het kader van zijn akkoord, zal het BIPT nagaan of de instantie wel degelijk gekwalificeerd en onafhankelijk is.
Cependant, cet auditeur ne pourra pas prendre connaissance du journal de l'opérateur ou de demandes d'accès des autorités, et ce afin de protéger la confidentialité de ces demandes.	Toch zal deze auditor geen kennis kunnen nemen van het logboek van de operator of de verzoeken om toegang vanwege de autoriteiten, teneinde de vertrouwelijkheid van deze verzoeken te vrijwaren.
Art. 12	Art. 12
Pour une plus grande lisibilité de la loi, l'ancien article 126/1 de la LCE a été déplacé vers l'article 127/3 de la même loi. Quelques modifications ont été apportées à cet article.	Om de wet leesbaarder te maken is het oude artikel 126/1 van de WEC verplaatst naar artikel 127/3 van dezelfde wet. In dat artikel zijn enkele wijzigingen aangebracht.
Tout d'abord, au paragraphe 1er, vu que la notion de service de communications électroniques est définie dans le Code de manière plus large qu'actuellement, il n'est plus nécessaire de viser dans l'article 127/3 les opérateurs et les fournisseurs de service mais il suffit de viser les opérateurs.	Allereerst, in paragraaf 1, aangezien de notie van elektronische-communicatiedienst in het Wetboek ruimer gedefinieerd is dan nu het geval is, is het niet meer noodzakelijk om in artikel 127/3 de operatoren en de aanbieders van diensten te beogen, maar volstaat het om de operatoren te beogen.
L'alinéa 1er renvoyait à une liste de dispositions (« des articles 46bis, 88bis et 90ter du Code d'instruction criminelle, des articles 18/7, 18/8, 18/16 et 18/17 de la loi du 30 novembre 1998 organique des services de	Het eerste lid verwees naar een lijst van bepalingen ("de artikelen 46bis, 88bis en 90ter van het Wetboek van strafvordering, de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 houdende

renseignement et de sécurité et des articles 81, 82, 2°, et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers »), qui, avec le temps, est devenue longue et incomplète. Cette liste est remplacée par une référence aux pouvoirs des autorités de demander aux opérateurs fournissant des services de communications électroniques en Belgique des données relatives aux communications électroniques.	regeling van de inlichtingen- en veiligheidsdiensten en de artikelen 81, 82, 2°, en 84, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten”) die in de loop van de tijd lang en onvolledig is geworden. Deze lijst wordt vervangen door een verwijzing naar de bevoegdheden van de autoriteiten om aan de operatoren die in België elektronische-communicatiediensten verstrekken, gegevens met betrekking tot de elektronische communicatie te mogen vragen.
Afin de protéger les données et dans un but d'efficacité, il est essentiel que les différentes autorités qui entendent obtenir de l'opérateur des données de communications électroniques s'adressent à sa Cellule de coordination. Cela peut se mettre en œuvre par un système automatisé de demandes envers la Cellule et de réponses automatiques de cette dernière.	Teneinde de data te beschermen en met het oog op efficiëntie, is het essentieel dat de verschillende autoriteiten die van de operator elektronische-communicatiegegevens horen te krijgen, zich richten tot diens Coördinatiecel. Dat kan verlopen via een geautomatiseerd systeem van verzoeken aan de Cel en automatische antwoorden van deze laatste.
Certaines exigences qui se trouvaient auparavant dans l'article 126/1, paragraphe 1er, (avis de sécurité et communication des coordonnées des membres de la Cellule de coordination à l'Autorité de protection des données et à l'IBPT) ont été supprimées, étant donné qu'elles seront dorénavant réglées par arrêté royal. Il s'agit en effet d'aspects pratiques qui mettent en œuvre les principes d'accessibilité et de fiabilité du personnel des opérateurs traitant les demandes des autorités.	Sommige eisen die voordien opgenomen waren in artikel 126/1, paragraaf 1, (veiligheidsadvies en mededeling van de contactgegevens van de leden van de Coördinatiecel aan de Gegevensbeschermingsautoriteit en aan het BIPT) zijn opgeheven, aangezien ze voortaan bij koninklijk besluit worden geregeld. Het gaat immers om praktische aspecten die de principes toepassen inzake toegankelijkheid en betrouwbaarheid van het personeel van de operatoren die de vorderingen van de autoriteiten behandelen.
La communication des coordonnées de la Cellule de coordination aux autorités sera dorénavant réglée par arrêté royal.	De mededeling van de contactgegevens van de Coördinatiecel aan de autoriteiten, zal voortaan vastgelegd zijn bij koninklijk besluit.
La référence à l'article 114 de la loi télécom a été supprimée, étant donné que l'article 127/2, § 3, alinéa 2, 2°, fait dorénavant référence à l'article équivalent de la même loi après la transposition du code des communications électroniques européen..	De verwijzing naar artikel 114 van de telecomwet werd verwijderd, aangezien artikel 127/2, § 3, tweede lid, 2°, voortaan verwijst naar het gelijkwaardige artikel van dezelfde wet na de omzetting van het Europees wetboek voor elektronische communicatie..
Les anciens articles 126/1 et 127 indiquaient que l'opérateur est le responsable du traitement. De manière simplifier la législation, c'est dorénavant l'article 127/3 qui reprend les différents articles pour lesquels l'opérateur est	De voormalige artikelen 126/1 en 127 duiden de operator aan als verantwoordelijke voor de verwerking. Om de wetgeving te vereenvoudigen, is het voortaan artikel 127/3 dat de verschillende artikelen overneemt

considéré comme le responsable du traitement.	waarvoor de operator als verantwoordelijke van de verwerking wordt beschouwd.
Cette disposition est sans préjudice d'autres hypothèses pour lesquelles l'opérateur doit également être qualifié de responsable du traitement.	Deze bepaling doet geen afbreuk aan andere hypothesen waarvoor de operator ook als verantwoordelijke voor de verwerking moet aangemerkt zijn.
Ensuite, au paragraphe 3, la fonction de préposé à la protection des données à caractère personnel a été supprimée pour la raison suivante. Cette fonction a dû être introduite dans l'article 126/1 par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, vu que les opérateurs ne devaient pas encore désigner un délégué à la protection des données en vertu du RGPD. Vu que ce dernier est entretemps entré en vigueur et que tout opérateur doit, conformément à l'article 37.1.(b) du RGPD, disposer d'un délégué à la protection des données, les missions du délégué au sens de l'ancien article 126/1 de la loi télécom tombent dorénavant dans les missions du délégué à la protection des données au sens du RGPD.	Vervolgens, in paragraaf 3 is de functie van aangestelde voor de bescherming van de persoonsgegevens geschrapt om de volgende reden. Die functie moest worden ingevoerd in artikel 126/1 bij de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, aangezien de operatoren nog geen functionaris voor gegevensbescherming moesten aanwijzen krachtens de AVG. Vermits die verordening inmiddels in werking is getreden en elke operator, conform artikel 37.1 (b) van de AVG over een functionaris voor gegevensbescherming moet beschikken, vallen de opdrachten in de zin van het oude artikel 126/1 van de telecomwet van die aangestelde voortaan binnen de opdrachten van de functionaris voor gegevensbescherming in de zin van de AVG.
Les délégations au Roi prévues dans l'ancien article 127, § 1er, et l'ancien article 126/1, § 4, qui permettaient à ce dernier de régler la collaboration entre les opérateurs et les autorités pour la fourniture de données à ces dernières ont été réécrites dans l'article 127/3, paragraphe 3.	De delegaties aan de Koning vastgelegd in het voormalige artikel 127, § 1, en het voormalige artikel 126/1, § 4, die deze laatste in staat stelden om de samenwerking tussen de operatoren en de autoriteiten voor de verstrekking van gegevens aan deze laatste te regelen, werden herschreven in artikel 127/3, paragraaf 3.
Au paragraphe 3 (anciennement le paragraphe 4), les délégations au Roi visent dorénavant l'avis des autorités de protection de données à caractère personnel et non plus l'avis de la Commission pour la protection de la vie privée. Il ne peut en effet pas être exclu que l'arrêté royal d'exécution de l'article 127/1 comprenne certaines dispositions qui règlent le fonctionnement des services de police ou des services de renseignement et de sécurité, pour autant que cela ait un impact sur la collaboration des opérateurs avec ces autorités. Dans ce cas, l'Organe de Contrôle de l'information policière et le Comité I devront également rendre leur avis sur ces dispositions.	In paragraaf 3 (voordien paragraaf 4) doelen de delegaties aan de Koning voortaan op het advies van de gegevensbeschermingsautoriteiten en niet langer op het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Het kan immers niet worden uitgesloten dat het koninklijk besluit ter uitvoering van artikel 127/1 enkele bepalingen bevat die de werking van de politiediensten of van de inlichtingen- en veiligheidsdiensten regelen, voor zover dat een impact heeft op de medewerking van de operatoren met die autoriteiten. In dat geval zullen het Controleorgaan op de politionele informatie en het Comité I ook hun advies over die bepalingen moeten verstrekken.

<p>L'article 22quinquies de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité prévoit une procédure au terme de laquelle l'Autorité Nationale de Sécurité (ANS) prend une décision d'imposer un avis de sécurité pour des catégories de personnes au sein de certaines organisations. Le présent article déroge à cette procédure, vu qu'il permet au Roi d'imposer à certaines catégories d'opérateurs un avis de sécurité pour les membres de la Cellule de coordination.</p>	<p>Artikel 22quinquies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen voorziet in een procedure na afloop waarvan de Nationale Veiligheidsoverheid (NVO) een beslissing neemt om een veiligheidsadvies op te leggen voor categorieën van personen bij sommige organisaties. Het onderhavige artikel wijkt af van deze procedure, aangezien het de Koning in staat stelt om aan bepaalde categorieën van operatoren een veiligheidsadvies op te leggen voor de leden van de Coördinatiecel.</p>
<p>Depuis sa modification par la loi du 2 mai 2019, l'article 22quinquies, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité prévoit une obligation à charge d'une entreprise de désigner un officier de sécurité lorsque certains membres du personnel de cette entreprise sont soumis à un avis de sécurité positif.</p>	<p>Sedert de wijziging ervan bij de wet van 2 mei 2019 voorziet artikel 22quinquies, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen in een verplichting in hoofde van een onderneming om een veiligheidsofficier aan te wijzen wanneer sommige personeelsleden van die onderneming onderworpen zijn aan een positief veiligheidsadvies.</p>
<p>Cette obligation n'a cependant pas été conçue dans le contexte de la Cellule de coordination des opérateurs et s'avère être disproportionnée pour les opérateurs qui ne reçoivent pas ou peu de demandes des autorités judiciaires ou des services de renseignement et de sécurité relatives aux données de communications électroniques.</p>	<p>Deze verplichting is echter niet bedacht in de context van de Coördinatiecel van de operatoren en blijkt onevenredig te zijn voor de operatoren die van de gerechtelijke autoriteiten of van de inlichtingen- en veiligheidsdiensten geen of weinig verzoeken ontvangen in verband met de elektronische-communicatiegegevens.</p>
<p>Dès lors, si le Roi impose au(x) membre(s) de la Cellule de coordination de faire l'objet d'un avis de sécurité, Il identifiera les catégories d'opérateurs qui sont dispensés de l'obligation de disposer d'un officier de sécurité et, si nécessaire, pourra fixer les règles à suivre du fait de l'absence d'un tel officier.</p>	<p>Daarom zal, indien de Koning aan het lid of de leden van de Coördinatiecel de verplichting oplegt om het voorwerp uit te maken van een veiligheidsadvies, Hij de categorieën van operatoren identificeren die vrijgesteld zijn van de verplichting om over een veiligheidsofficier te beschikken en indien nodig, zal Hij de regels kunnen vaststellen die gevolgd moeten worden wegens het ontbreken van zo'n officier.</p>
<p>La délégation au Roi dans le paragraphe 3, 4°, permettra d'organiser la manière dont les coordonnées de la cellule de coordination et de ses membres sont portées à la connaissance des autorités belges qui ont besoin de ces informations. En pratique et à l'heure actuelle, la communication de ces</p>	<p>De delegatie aan de Koning in paragraaf 3, 4°, zal het mogelijk maken om de manier te organiseren waarop de contactgegevens van de Coördinatiecel en van de leden ervan, ter kennis worden gebracht van de Belgische autoriteiten, die deze informatie nodig hebben. In de praktijk en op dit ogenblik geschiedt de mededeling van die</p>

coordonnées se fait par le biais d'un outil informatique mis en place par l'IBPT.	contactgegevens via een computerprogramma dat door het BIPT is ingesteld.
Pour une meilleure lisibilité de la LCE, le paragraphe 3, 5°, reprend les éléments de l'ancien article 127 qui concernent la collaboration entre les opérateurs et les autorités belges, pour ce qui concerne l'obtention des données relatives aux communications électroniques, en particulier la fixation des tarifs dans le cadre de cette collaboration. Ce paragraphe a également été retravaillé pour expliquer les principaux éléments que le Roi doit encore régler.	Voor een betere leesbaarheid van de WEC neemt paragraaf 3, 5°, de elementen over van het oude artikel 127 die betrekking hebben op de samenwerking tussen de operatoren en de Belgische overheid, wat betreft het verkrijgen van de elektronische-communicatiegegevens, in het bijzonder de vaststelling van de tarieven in het kader van die samenwerking. Deze paragraaf is eveneens herwerkt om de voornaamste elementen uit te leggen die de Koning nog moet regelen.
Dans l'arrêté royal d'exécution de l'article 127/3, § 3, le Roi pourra, si c'est justifié, prévoir des règles différentes selon différentes catégories d'opérateurs, de manière à prendre en compte les situations différentes dans lesquelles ils se trouvent.	In het koninklijk besluit ter uitvoering van artikel 127/3, § 3, zal de Koning, indien dat gerechtvaardigd is, verschillende regels kunnen vaststellen volgens verschillende categorieën van operatoren, om rekening te houden met de uiteenlopende situaties waarin zij zich bevinden.
Art. 13	Art. 13
L'article 127/4 de la loi télécom reprend tel quel l'ancien article 9, § 7, de la même loi.	Artikel 127/4 van de telecomwet neemt het oude artikel 9, § 7, van dezelfde wet over.
Par ailleurs, cet article a été mis en conformité avec l'arrêt Quadrature du Net du 6/10/2020 de la CJUE (aff. jointes C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.). En effet, l'article ne se réfère plus à l'enregistrement et la conservation des données de trafic mais des données permettant l'identification des personnes qui utilisent le service de communications électroniques, de l'équipement terminal ou du service de communications électroniques employé..	Overigens werd dat artikel afgestemd op het arrest-Quadrature du Net van 6/10/2020 van het HvJ-EU (gevoegde zaken C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.). Het artikel verwijst inderdaad niet langer naar de registratie en bewaring van de verkeersgegevens maar naar gegevens die de identificatie mogelijk maken van de personen die de elektronische-communicatiedienst gebruiken, de eindapparatuur of de gebruikte elektronische-communicatiedienst..
Cet article ajoute une référence vers les articles 464/13, 464/25 et 464/26 du Code d'instruction criminelle, qui concernent l'enquête pénale d'exécution, vu que ces articles sont liés aux articles 46bis, 88bis et 90ter qui étaient déjà cités dans l'article 9, § 7.	Dit artikel voegt een verwijzing toe naar de artikelen 464/13, 464/25 en 464/26 van het Wetboek van Strafvordering, die handelen over het strafrechtelijk uitvoeringsonderzoek, aangezien deze artikelen verband houden

	met de artikelen 46bis, 88bis en 90ter die reeds geciteerd waren in artikel 9, § 7.
Art. 14	Art. 14
Cet article 127/5 reprend certains éléments de l'ancien article 127.	Dit artikel 127/5 neemt bepaalde elementen over van het oude artikel 127.
L'alinéa 1er du paragraphe 1er prévoit que les règles prévues dans cet alinéa ne sont pas applicables pour les systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements. En effet, ces systèmes d'encryptage font l'objet de règles spécifiques dans le paragraphe 2.	Het eerste lid van paragraaf 1 bepaalt dat de in dit lid vastgestelde regels niet van toepassing zijn op versleutelingssystemen die gebruikt kunnen worden om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen. Deze versleutelingssystemen vallen immers onder specifieke regels in paragraaf 2.
Une opération a été ajoutée dans la liste que comprend cet article, à savoir la fourniture des données d'identification de l'appelant au bénéfice des services d'urgence qui offrent de l'aide sur place. L'accès à ces services est en effet d'importance vitale.	In de lijst die in dat artikel staat wordt een verrichting toegevoegd, namelijk de levering van de identificatiegegevens van de oproeper ten voordele van de nooddiensten die ter plaatse hulp bieden. De toegang tot deze diensten is immers van levensbelang.
Les systèmes d'encryptage se révèlent être des outils efficaces pour garantir un niveau élevé de confidentialité des communications ainsi que de sécurité des paiements. Par principe, ils doivent donc être encouragés, en ce compris ceux mis en place par les opérateurs.	Encryptiesystemen blijken doeltreffende tools te zijn om een hoog niveau van vertrouwelijkheid van de communicatie alsook van de veiligheid van de betalingen te garanderen. Ze moeten dus principieel worden aangemoedigd, ook deze ingevoerd door de operatoren.
A cet égard, l'article 105/4 de la loi (l'article 48 avant la transposition dans la loi télécom du Code des communications électroniques européen) précise que « L'emploi de la cryptographie est libre ». Cet article avait initialement été inséré dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (à l'article 109ter F) suite à la libéralisation du secteur des télécommunications. L'exposé des motifs de la loi du 19 décembre 1997 précisait la nécessité de cette insertion comme suit : « Ceci est nécessaire afin de montrer l'évolution par rapport à la législation précédente qui entendait soumettre la cryptographie à des	In dat opzicht bepaalt artikel 105/4 van de wet (artikel 48 vóór de omzetting van het Europees wetboek voor elektronische communicatie in de telecomwet): "Het gebruik van versleuteling is vrij". Dat artikel was aanvankelijk ingevoegd in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (in artikel 109ter F) na de liberalisering van de telecomunicatiesector. De memorie van toelichting bij de wet van 19 december 1997 verduidelijkte de noodzaak tot deze invoeging als volgt: "Dit is nodig om de ontwikkeling aan te tonen ten opzichte van de voorgaande wetgeving die de versleuteling aan

<p>procédures de dépôt de clés. En effet, l'état de l'art ne permet pas la mise en œuvre d'un tel système à l'heure actuelle. Dès lors, étant entendu que la cryptographie est nécessaire au développement du commerce sur les autoroutes de l'information et à une meilleure protection des données à caractère personnel, il est apparu nécessaire de faciliter l'usage de ces techniques. Ceci ne signifie pas que le législateur ait complètement abandonné toute volonté de pouvoir à l'avenir avoir accès aux messages en clair lorsque des écoutes judiciaires ont été autorisées. Cette problématique sera revue plus tard au vu de l'évolution de la technologie ou d'un usage abusif de la cryptographie par des structures mafieuses ou terroristes. » (Parl. Chambre, 49-1265/1, p. 55).</p>	<p>procedures wilde onderwerpen in verband met de neerlegging van sleutels. Technisch is de verwezenlijking van een dergelijk systeem momenteel in feite onmogelijk. Vandaar dat het noodzakelijk is gebleken om het gebruik van die technieken te vergemakkelijken aangezien versleuteling nodig is voor de ontwikkeling van de handel op de informatiesnelwegen en voor een betere bescherming van de persoonsgebonden gegevens. Dit betekent niet dat de wetgever volledig alle wil heeft laten varen om in de toekomst toegang te hebben tot ongecodeerde berichten, wanneer toestemming is verleend voor af luistering door het gerecht. Die problematiek zal later worden herzien gelet op de ontwikkeling van de technologie of van misbruik van de versleuteling door maffiaorganisaties of terroristen." (Parl. Kamer, 49-1265/1, blz. 55).</p>
<p>Le paragraphe 2 de l'article 127/5 apporte une série de dérogations à l'article 105/4.</p>	<p>Paragraaf 2 van artikel 127/5 brengt een reeks afwijkingen van artikel 105/4 aan.</p>
<p>Tout d'abord, les systèmes d'encryptage ne peuvent pas avoir pour effet d'empêcher les communications d'urgence (paragraphe 1er, alinéa 1er, 1°). Par contre, le paragraphe 1er, alinéa 1er, 2° et 3°, n'est pas applicable aux systèmes d'encryptage, de sorte que ces systèmes restent autorisés.</p>	<p>Allereerst mogen de versleutelingssystemen niet tot gevolg hebben dat noodcommunicatie wordt verhinderd (paragraaf 1, eerste lid, 1°). Paragraaf 1, eerste lid, 2° en 3° is daarentegen niet van toepassing op de versleutelingssystemen, zodat die systemen toegestaan blijven.</p>
<p>Ces systèmes ne peuvent pas avoir pour effet qu'un opérateur n'est plus en mesure de conserver les données d'identification, de trafic ou de localisation pour les autorités comme prévu dans la loi télécom, le Code d'instruction criminelle ou la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.</p>	<p>Deze systemen mogen niet tot gevolg hebben dat een operator niet langer in staat is om de identificatie-, verkeers- of locatiegegevens te bewaren voor de autoriteiten zoals voorgeschreven in de telecomwet, het Wetboek van Strafvordering of de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.</p>
<p>Comme l'avait anticipé le législateur de 1997, la pratique révèle que les organisations criminelles ont largement recours aux systèmes de cryptographie de manière à échapper aux mesures d'interception légale qui pourraient être prises à leur égard.</p>	<p>Zoals de wetgever in 1997 had voorzien, uit de praktijk blijkt dat criminele organisaties in ruime mate gebruikmaken van versleutelingssystemen om te ontsnappen aan de maatregelen inzake wettelijke onderschepping die tegen hen zouden kunnen worden genomen.</p>
<p>Une conciliation de ces intérêts s'avère donc nécessaire, de manière à ce que ces mesures d'interception légale puissent continuer à</p>	<p>Die belangen dienen dus met elkaar te worden verzoend zodat deze maatregelen inzake wettelijke onderschepping hun doel</p>

remplir leur objectif, sans nuire à la généralisation de l'emploi de la cryptographie dans un but de confidentialité des communications et de sécurité des paiements, ni à sa fiabilité.	kunnen blijven vervullen, zonder te raken aan het veralgemeende gebruik van versleuteling met het oog op de vertrouwelijkheid van de communicatie en de veiligheid van betalingen, noch aan de betrouwbaarheid daarvan.
En particulier, lorsqu'un opérateur permet, à l'aide de son réseau et sur base d'un accord de roaming, l'utilisation en Belgique de cartes SIM étrangères, il est essentiel que les systèmes de cryptographie mis en place par l'opérateur (belge ou étranger) ne puissent pas avoir pour conséquence d'empêcher la réalisation de mesures d'interception légale aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	Wanneer een operator echter specifiek, aan de hand van zijn netwerk en op basis van een roamingovereenkomst, het gebruik van buitenlandse simkaarten in België toestaat, is het van essentieel belang dat de encryptiesystemen die de (Belgische of buitenlandse) operator heeft ingevoerd, niet als gevolg kunnen hebben dat ze de uitvoering verhinderen van maatregelen van wettelijke onderschepping volgens de voorwaarden vastgelegd in het Wetboek van Strafvordering en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.
En toute hypothèse, l'opérateur belge notifié à l'IBPT en vertu de l'article 9 de la loi télécom doit pouvoir faire droit dans les [24 heures] de la transmission de la requête aux mesures d'interception légale des autorités belges, même lorsqu'il fournit un service de roaming à un opérateur étranger (carte SIM étrangère utilisée en Belgique).	In elk geval moet een Belgische operator die krachtens artikel 9 van de telecomwet genotificeerd is aan het BIPT, binnen [24 uur] na de verzending van het verzoekschrift gevolg kunnen geven aan de maatregelen inzake wettelijke onderschepping van de Belgische autoriteiten, zelfs wanneer hij een roamingdienst verstrekt aan een buitenlandse operator (buitenlandse simkaart die in België wordt gebruikt).
Il appartient aux opérateurs de déterminer les solutions concrètes les plus adaptées afin de veiller à ce que les mesures d'interception légale soient rendues possibles, nonobstant l'utilisation de systèmes de cryptographie, et uniquement pour les communications visées dans la requête (en particulier les limitations aux personnes ou identifiants visés dans la requête ainsi qu'à la période sur laquelle l'interception porte visée dans la requête).	Het is aan de operatoren om de meest gepaste concrete oplossingen te bepalen teneinde ervoor te zorgen dat de maatregelen van wettelijke onderschepping kunnen worden uitgevoerd ondanks het gebruik van encryptiesystemen en enkel voor de communicatie bedoeld in het verzoekschrift (in het bijzonder de beperkingen tot de personen of identificatoren bedoeld in het verzoekschrift, alsook tot de periode waarop de in het verzoekschrift bedoelde onderschepping betrekking heeft).
Afin de garantir l'effectivité de cette limite à l'autorisation de principe de l'utilisation des systèmes de cryptographie, il est prévu que toute clause contractuelle faisant obstacle au respect de cette obligation est interdite et nulle.	Opdat deze beperking van de principiële toestemming om encryptiesystemen te gebruiken doeltreffend zou zijn, wordt bepaald dat elke contractuele clausule die de inachtneming van deze verplichting belemmert, verboden en nietig is.

Art. 15	Art. 15
La liste des articles dont le non-respect est puni pénalement est adaptée aux nouveaux articles qui ont pour objectif la fourniture de données de communications électroniques aux autorités.	De lijst van de artikelen waarvan de niet-inachtneming strafrechtelijk wordt bestraft, is aangepast aan de nieuwe artikelen met als doel de verstrekking van elektronische-communicatiegegevens aan de autoriteiten.
Par ailleurs, le paragraphe 3ter de l'article 145, annulé par la Cour constitutionnelle dans son arrêt n° 57/2021, a été réintroduit. Il est en effet essentiel que des sanctions pénales soient prévus en cas d'abus lors de l'accès aux données de trafic conservées par les opérateurs pour les autorités.	Paragraaf 3ter van artikel 145, die werd vernietigd door het Grondwettelijk Hof in zijn arrest nr. 57/2021, werd overigens opnieuw ingevoegd. Het is immers van essentieel belang dat er wordt voorzien in strafsancities in geval van misbruik bij inzage in de verkeersgegevens die de operatoren bewaren voor de autoriteiten.
CHAPITRE 3 - Modifications à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.	HOOFDSTUK 3 – Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector
Art. 16	Art. 16
La disposition insérée vise à permettre à l'Institut d'avoir accès aux données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, lorsque cela s'avère nécessaire à l'accomplissement de l'une de ses missions.	De ingevoegde bepaling beoogt dat het Instituut toegang kan hebben tot de identificatie-, verkeers- of locatiegegevens in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, wanneer dat nodig blijkt voor de vervulling van een van zijn opdrachten.
Tel est le cas notamment en cas de contrôle du respect par les opérateurs de leurs obligations légales, telles que l'obligation d'adresser une facturation détaillée, prévue à l'article 110 de la loi du 13 juin 2005 relative aux communications électroniques, ou dans le cadre de la mise en œuvre de	Dat is met name het geval bij de controle van de inachtneming door de operatoren van hun wettelijke verplichtingen zoals de verplichting om een gedetailleerde facturering op te stellen, vastgelegd in artikel 110 van de wet van 13 juni 2005 betreffende de elektronische communicatie, of in het

l'article 114 de cette même loi. Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées.	kader van de tenuitvoerbrenging van artikel 114 van diezelfde wet. Zo moet het BIPT, in het geval van de gedetailleerde facturering, in staat zijn om een operator een staal van zijn facturen te vragen. Deze facturen bevatten verkeersgegevens, zoals de ontvangers, data, tijdstippen en duur van de gevoerde gesprekken.
CHAPITRE 4 - Modifications du Code d'instruction criminelle	HOOFDSTUK 4 - Wijzigingen aan het Wetboek van strafvordering
Art. 17	Art. 17
Cette disposition introduit un nouvel article 39quinquies dans le Code d'instruction criminelle, qui permet au procureur du Roi d'ordonner, lors de la recherche de crimes et délits, la conservation de certaines données de trafic et de localisation pour les besoins de l'enquête.	Deze bepaling voert een nieuw artikel 39quinquies in het Wetboek van Strafvordering in, op grond waarvan de procureur des Konings de bewaring van bepaalde verkeers- en locatiegegevens kan bevelen tijdens het onderzoek van misdaden en wanbedrijven.
Suite à l'arrêt de la Cour constitutionnelle n°57/2021 du 22 avril 2021, il n'existe plus d'obligation de conservation générale et indifférenciée de toutes les données de trafic et de localisation à des fins de recherche et de poursuite d'infractions pénales.	Ten gevolge van het arrest nr. 57/2021 van het Grondwettelijk Hof van 22 april 2021, bestaat er niet langer een algemene en ongedifferentieerde verplichting om alle verkeers- en locatiegegevens te bewaren met het oog op de opsporing en de vervolging van strafbare feiten.
Or, ces données jouent un rôle de plus en plus essentiel dans les enquêtes pénales, ce qui s'explique par l'utilisation croissante des nouvelles technologies. Par exemple, l'accès aux données de communication est une étape incontournable pour identifier des personnes et les liens entre celles-ci.	Deze gegevens spelen echter een steeds essentiëlere rol in strafrechtelijke onderzoeken, hetgeen te wijten is aan het toenemend gebruik van nieuwe technologieën. Zo is toegang tot communicatiegegevens een essentiële stap bij het identificeren van personen en de banden tussen hen.
Les données de communication sont souvent nécessaires pour la recherche et la poursuite d'une grande variété d'infractions comme le terrorisme, la pédopornographie, le trafic de stupéfiants, le harcèlement, le piratage de comptes bancaires, le vol d'identité, les incitations à la haine ou à la	Communicatiegegevens zijn vaak noodzakelijk voor het onderzoek naar en de vervolging van een breed scala van strafbare feiten, zoals terrorisme, kinderpornografie, drugshandel, belaging, hacken van bankrekeningen, identiteitsdiefstal, aanzetten tot haat of

violence, ... (Doc. Parl., Chambre, n° 54-1567/001, p. 5-6).	geweld, ... (Parl. St., Kamer, nr. 54-1567/001, blz. 5-6).
Sans la conservation généralisée et indifférenciée de ces données, de nombreuses données pourraient ne pas être disponibles, ce qui pourrait être extrêmement dommageable dans certaines enquêtes, où des éléments de preuves qui pourraient s'avérer essentiels seront dès lors perdus.	Zonder de algemene en ongedifferentieerde bewaring van dergelijke gegevens is het mogelijk dat vele gegevens niet beschikbaar zijn, hetgeen in sommige onderzoeken uiterst schadelijk kan zijn, omdat potentieel essentieel bewijsmateriaal verloren zal gaan.
C'est dans cette optique que le nouvel article 39quinquies vient en complément, dans le cadre spécifique de la recherche de délits et de crimes, d'autres mesures de conservation des données de trafic et de localisation, telles que la conservation ciblée préventive de données afférentes à certaines zones géographiques.	In deze optiek vormt het nieuwe artikel 39quinquies, in de specifieke context van het onderzoek naar wanbedrijven en misdaden, een aanvulling op andere maatregelen voor de bewaring van verkeers- en locatiegegevens, zoals de gerichte preventieve bewaring van gegevens betreffende bepaalde geografische gebieden.
Bien que cette nouvelle mesure ne permette pas de remonter dans le passé puisqu'elle intervient dans le cadre d'une enquête spécifique, l'alinéa 1 ^{er} du paragraphe 1 de l'article 39quinquies permet néanmoins au procureur du Roi d'ordonner, dans certaines conditions et selon certaines modalités, aux opérateurs la conservation de certaines données qui pourraient être essentielles pour les besoins de l'enquête.	Hoewel met deze nieuwe maatregel niet naar het verleden kan worden teruggerepen, aangezien deze in het kader van een specifiek onderzoek wordt toegepast, kan de procureur des Konings op grond van artikel 39quinquies, § 1, eerste lid, onder bepaalde voorwaarden en volgens bepaalde procedures, de bewaring bevelen van bepaalde gegevens die van essentieel belang kunnen zijn voor het onderzoek.
Une de ces conditions est que cette mesure ne peut être prise que s'il existe des indices sérieux que les infractions puissent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde.	Een van deze voorwaarden is dat de maatregel enkel genomen kan worden als er sterke aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben.
Ainsi, le gouvernement veut s'assurer que cette mesure ne s'applique que dans le cadre de la recherche et de la poursuite d'infractions d'une certaine gravité.	Zo wil de regering ervoor zorgen dat deze maatregel alleen geldt voor de opsporing en vervolging van strafbare feiten van een zekere ernst.
Puis, l'obligation de conservation ne concerne que les données de trafic et de localisation visées à l'article 88bis, § 1er, alinéa 1er du Code d'instruction criminelle, soit :	Vervolgens heeft de verplichting tot bewaring slechts betrekking op de verkeers- en locatiegegevens bedoeld in artikel 88bis, § 1, eerste lid, van het Wetboek van Strafvordering, dat wil zeggen :
« 1° les données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des	« 1° de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan; »

<i>communications électroniques sont adressées ou ont été adressées; »</i>	
<i>« 2° les données de localisation de l'origine ou de la destination de communications électroniques. »</i>	<i>« 2° de gegevens betreffende de oorsprong of de bestemming van elektronische communicatie. »</i>
Le procureur du Roi doit limiter son réquisitoire aux seules données qui sont susceptibles de contribuer à l'élucidation de l'infraction.	De procureur des Konings moet zijn vordering beperken tot enkel die gegevens die kunnen bijdragen tot de opheldering van het strafbare feit.
Enfin, la décision doit être écrite et motivée.	Ten slotte moet de beslissing schriftelijk en met redenen omkleed zijn.
L'alinéa 2 du paragraphe 1er détermine les acteurs qui peuvent, sur ordre du procureur du Roi, directement ou par l'intermédiaire d'un service de police désigné par le Roi, être obligés de conserver les données.	Het tweede lid van de eerste paragraaf bepaalt welke actoren door de procureur des Konings, rechtstreeks of door tussenkomst van een door de Koning aangewezen politiedienst, kunnen worden gevorderd de gegevens te bewaren.
Ces acteurs sont tout opérateur d'un réseau de communications électroniques, ainsi que 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.	Deze actoren zijn elke operator van een elektronisch communicatienetwerk, alsmede iedereen die binnen het Belgische 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 om informatie te verkrijgen, te ontvangen of te verspreiden via een elektronisch communicatienetwerk.
Cette définition est prise de l'arrêt Yahoo (arrêt de la Cour de cassation du 18/01/2011). A l'instar des articles 46bis, 88bis, 90quater, 464/13 et 464/25 du Code d'instruction criminelle qui reprennent cette définition, il est ajouté dans un souci de clarté « <i>Est également compris le fournisseur d'un service de communications électroniques.</i> »	Deze definitie is overgenomen uit het Yahoo-arrest (arrest van het Hof van Cassatie van 18/01/2011). Naar het voorbeeld van de artikelen 46bis, 88bis, 90quater, 464/13 en 464/25 van het wetboek van strafvordering, waarin deze definitie is opgenomen, wordt omwille van de duidelijkheid het volgende toegevoegd: « <i>Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.</i> »
L'alinéa 3 du premier paragraphe énonce les mentions qui doivent figurer dans la décision du procureur du Roi.	In het derde lid van de eerste paragraaf wordt bepaald welke vermeldingen in de beslissing van de procureur des Konings moeten worden opgenomen.
Ces mentions sont inspirées de l'article 39ter du CIC.	Deze vermeldingen zijn gebaseerd op artikel 39ter van het W.Sv.

<p>Il est à noter que la décision doit indiquer précisément la ou les personnes, le(s) lieu(x) ou les moyens de communications qui font l'objet de la conservation. La mesure ne concerne pas seulement les données afférentes au suspect, il peut s'agir de données afférentes à la victime, à son entourage social ou professionnel, à des lieux déterminés, telles que les lieux de la commission et/ou de la préparation de l'infraction, ou encore à des moyens de communication.</p>	<p>Er moet op gewezen worden dat in de beslissing specifiek moet worden aangegeven op welke perso(n)en, plaats(en) of communicatiemiddel(en) de bewaring betrekking heeft. De maatregel heeft niet alleen betrekking op gegevens betreffende de verdachte, maar kan ook gegevens omvatten betreffende het slachtoffer, diens sociale of professionele kring, specifieke plaatsen, zoals de plaatsen waar het strafbare feit is gepleegd en/of voorbereid, of communicatiemiddelen.</p>
<p>Le procureur pourrait par exemple ordonner la mesure pour un périmètre autour de la maison où il y a eu un meurtre, ainsi que pour les personnes qui connaissaient la victime.</p>	<p>De procureur zou bijvoorbeeld de maatregel kunnen gelasten voor een perimeter rond het huis waar een moord heeft plaatsgevonden, alsook voor mensen die het slachtoffer hebben gekend.</p>
<p>Ou, il est constaté qu'un gang de motards faisant l'objet d'une enquête pénale a déplacé le club-house dans un lieu ne relevant pas du champ d'application de l'article 126/1 de la loi relative aux communications électroniques et qu'il y a donc un risque qu'il n'y ait pas de données de communication disponibles si jamais on en a besoin dans le cadre de l'enquête. A ce moment-là, le Procureur du Roi pourrait ordonner la mesure de conservation ciblée pour un périmètre autour de ce club-house.</p>	<p>Of er wordt vastgesteld dat een motorbende tegen wie een strafrechtelijk onderzoek loopt, het clubhuis heeft verplaatst naar een locatie die buiten de werkingssfeer valt van artikel 126/1 van de wet betreffende de elektronische communicatie en dat er dus een risico bestaat dat de communicatiegegevens niet beschikbaar zullen zijn als zij ooit nodig zijn voor het onderzoek. Op dat moment kon de procureur des Konings opdracht geven tot de gerichte bewaringsmaatregel voor een perimeter rond dit clubhuis.</p>
<p>Il peut aussi s'agir de données recueillies par les services de police dans le cadre d'une information en cours indiquant qu'un enlèvement est projeté par une bande à l'encontre d'un mineur et dont la police a reçu via un indicateur un numéro de téléphone d'un auteur probable. A l'aide de cet unique numéro, et sur base de la conservation ciblée, en examinant les données de trafic et de localisation, on pourra essayer de déterminer les personnes actives dans cette bande pour in fine empêcher cet enlèvement.</p>	<p>Het kunnen ook gegevens zijn die door politiediensten worden verzameld in het kader van een lopend opsporingsonderzoek waaruit blijkt dat een bende een ontvoering van een minderjarige beraamt en waarbij de politie via een informant een telefoonnummer heeft gekregen van een vermoedelijke dader. Met behulp van dit ene nummer, en op basis van gerichte retentie, door het onderzoeken van de verkeers- en locatiegegevens, zal kunnen worden getracht de personen die actief zijn in deze bende te bepalen, om uiteindelijk deze ontvoering te voorkomen.</p>
<p>Le cas échéant, le procureur du Roi peut également indiquer dans sa décision pour quelles données ou catégories de données il demande la conservation ciblée. De cette manière, le magistrat peut limiter très clairement et spécifiquement la portée de sa</p>	<p>In voorkomend geval kan de procureur des Konings in zijn beslissing ook aanduiden voor welke gegevens of categorieën van gegevens hij de gerichte bewaring vraagt. Op die manier kan de magistrat heel duidelijk en gericht de draagwijdte van zijn</p>

<p>décision, également en la combinant avec une ou plusieurs des personnes, moyens de communication ou lieux visés mentionnés ci-dessus. Un procureur du Roi pourrait décider qu'il ne souhaite demander que la conservation de données de localisation, et donc pas de données relatives au trafic. Il peut aussi se limiter aux données générées par les pylônes qui assurent la couverture du trajet entre la résidence d'une cible et un hangar.</p>	<p>beslissing begrenzen, ook door de combinatie met een of meerdere van de hoger vermelde beoogde personen, communicatiemiddelen of plaatsen. Een procureur des Konings zou kunnen beslissen dat hij enkel de bewaring vraagt van locatiegegevens, en dus niet van verkeersgegevens. Of hij kan zich beperken tot de gegevens die gegenereerd worden door zendmasten die dekking geven aan het traject tussen de woonplaats van een target en een loods.</p>
<p>Le procureur du Roi pourra donc demander une conservation bien circonscrite en définissant précisément dans sa décision les personnes, les moyens de communication, les lieux et/ou les catégories de données auxquels sa décision s'applique.</p>	<p>De procureur des Konings zal dus een zeer goed omschreven bewaring kunnen vragen door in zijn beslissing precies te omschrijven op welke personen, communicatiemiddelen, plaatsen en/of categorieën van gegevens zijn beslissing van toepassing is.</p>
<p>La durée de la conservation des données est de 6 mois, renouvelable.</p>	<p>De duur van de bewaring van deze gegevens bedraagt 6 maanden, met mogelijkheid tot verlenging.</p>
<p>La durée de la mesure elle-même, c'est-à-dire la période pendant laquelle les opérateurs sont tenus de conserver les données, est de deux mois au maximum, sans préjudice d'un éventuel renouvellement de la mesure. Ce délai est conforme à ce qui est déjà prévu à l'article 88bis, § 1, alinéa 5 du code de procédure pénale. Ce délai doit également être mentionné dans la décision du procureur du Roi.</p>	<p>De duur van de maatregel zelf, dat wil zeggen de tijdsperiode gedurende dewelke de operatoren verplicht zijn de gegevens te bewaren, is maximum twee maanden, onverminderd een mogelijke hernieuwing van de maatregel. Deze termijn sluit aan bij wat al bepaald is in artikel 88bis, § 1, vijfde lid van het Wetboek van strafvordering. Deze termijn moet ook vermeld worden in de beslissing van de procureur des Konings.</p>
<p>L'alinéa 4 du paragraphe 1^{er} prévoit la possibilité, en cas d'urgence, d'ordonner verbalement la conservation des données. Dans ce cas, l'ordre doit être confirmé dans les plus brefs délais. Cette possibilité existe pour plusieurs mesures d'enquête – voir entre autres les articles 39ter, 46bis, 88bis. Dans ces articles, il est toujours mentionné que la confirmation écrite doit être donnée dans les plus brefs délais, sans préciser un délai concret. Dans la pratique, ces confirmations écrites ont lieu très rapidement, bien qu'il faille également tenir compte des week-ends, des jours fériés et des congés ainsi que des possibilités technologiques dont dispose le ministère public.</p>	<p>De vierde alinea van de eerste paragraaf voorziet in de mogelijkheid om in dringende gevallen een mondeling bevel tot bewaring van gegevens te geven. In dat geval moet de vordering zo spoedig mogelijk worden bevestigd. Deze mogelijkheid bestaat voor verscheidene onderzoeksmaatregelen - zie onder meer de artikelen 39 ter, 46 bis, 88bis. In die artikelen wordt telkens vermeld dat de schriftelijke bevestiging zo spoedig mogelijk dient te gebeuren, zonder daarbij een termijn te voorzien. In de praktijk gebeuren dergelijke schriftelijke bevestigingen zeer snel, al dient men hierbij ook rekening te houden met weekend-, feest-, en verlofdagen en met de technologische mogelijkheden waarover het openbaar ministerie beschikt.</p>

<p>Le paragraphe 2 requiert des opérateurs qu'ils conservent les données de manière sécurisée. A ce moment, les autorités judiciaires n'ont pas encore accès aux données. Le but de la mesure est justement de préserver les données pour que les autorités puissent y avoir accès ensuite par le biais de l'article 88bis du CIC. Ce paragraphe est repris en partie de l'article 39ter, § 2 du CIC.</p>	<p>De tweede paragraaf schrijft voor dat operatoren gegevens veilig moeten opslaan. Op dit ogenblik hebben de gerechtelijke autoriteiten nog geen toegang tot de gegevens. Het doel van de maatregel is juist om de gegevens te bewaren zodat de autoriteiten er later toegang toe kunnen krijgen op grond van artikel 88bis van het W. Sv. Deze paragraaf is gedeeltelijk overgenomen uit artikel 39ter, § 2, van het W. Sv.</p>
<p>Le paragraphe 3, alinéa 1 impose une obligation de confidentialité à toute personne qui a connaissance de la mesure. Cette obligation répond à un double objectif. D'une part, elle tient compte du bon déroulement de l'enquête. Il peut être important, surtout dans le cadre de l'information, que le suspect n'ait pas connaissance de l'enquête dont il est l'objet. Puis, la confidentialité permet également d'éviter que des personnes tentent de manipuler ou d'effacer des données. D'autre part, la confidentialité de la mesure permet de contribuer à défendre le droit à la vie privée des personnes pouvant être concernées par ces données.</p>	<p>Het eerste lid van de derde paragraaf legt aan eenieder die van de maatregel kennis heeft, een geheimhoudingsplicht op. Deze verplichting dient een tweeledig doel. Enerzijds wordt rekening gehouden met het goede verloop van het onderzoek. Het kan van belang zijn, met name in het kader van het opsporingsonderzoek, dat de verdachte geen kennis heeft van het tegen hem ingestelde onderzoek. Ten tweede helpt vertrouwelijkheid ook om te voorkomen dat mensen proberen gegevens te manipuleren of te wissen. Anderzijds draagt de vertrouwelijkheid van de maatregel bij tot de bescherming van het recht op privacy van personen die door de gegevens kunnen betrokken zijn.</p>
<p>L'alinéa 2 punit le refus de collaboration, ainsi que le fait d'altérer, de détruire ou de faire disparaître des données.</p>	<p>Het tweede lid bestraft de weigering om mee te werken, alsmede de wijziging, de vernietiging of het doen verdwijnen van gegevens.</p>
<p>Le paragraphe 3 est notamment repris des articles 46bis et 88bis qui imposent aussi une obligation de coopération aux opérateurs.</p>	<p>De derde paragraaf is overgenomen uit de artikelen 46bis en 88bis, die de operatoren eveneens een verplichting tot medewerking opleggen.</p>
<p>Enfin, le paragraphe 4 limite l'accès aux données conservées. Elles ne peuvent être transmises aux autorités judiciaires que par le biais de la mesure prévue à l'article 88bis du Code d'instruction criminelle. Il faut donc l'intervention d'un juge d'instruction, et les infractions doivent être de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. En limitant ainsi l'accès à ces données, le législateur veut éviter tout risque d'abus et d'accès illicite. L'accès à ces données est dès lors justifié par l'objectif d'intérêt général pour lequel la conservation a été imposée, soit la</p>	<p>Ten slotte wordt in de vierde paragraaf de toegang tot overeenkomstig dit artikel bewaarde gegevens beperkt. Zij kunnen alleen aan de gerechtelijke autoriteiten worden overgemaakt door middel van de maatregel voorzien in artikel 88bis van het Wetboek van Strafvordering. Hiervoor is de tussenkomst van een onderzoeksrechter vereist, en de strafbare feiten moeten van dien aard zijn dat zij aanleiding kunnen geven tot een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf. Door de toegang tot dergelijke gegevens op deze manier te</p>

recherche, la poursuite et la sanction d'infractions pénales graves.	beperken, wil de wetgever elk risico op misbruik en ongeoorloofde toegang vermijden. De toegang tot deze gegevens wordt derhalve gerechtvaardigd door het doel van algemeen belang waarvoor de bewaring is opgelegd, namelijk het onderzoeken, vervolgen en bestraffen van ernstige strafbare feiten.
Bien que cette mesure ne soit pas spécifiquement reprise comme piste de solution par la Cour de Justice de l'Union européenne, cette dernière a jugé dans son arrêt qu'il est loisible pour les états d'implémenter, sous certaines conditions, des modalités de conservations ciblées comme la conservation ciblée préventive et la conservation rapide.	Hoewel deze maatregel door het Hof van Justitie van de Europese Unie niet specifiek als mogelijke oplossing wordt genoemd, heeft het Hof in zijn arrest geoordeeld dat het de Lidstaten onder bepaalde voorwaarden is toegestaan om gerichte bewaringsmethoden toe te passen, zoals preventieve gerichte bewaring en snelle bewaring.
Concernant la conservation ciblée à titre préventif, la Cour indique au point 147 de l'arrêt du 06.10.20 :	Wat de preventieve gerichte bewaring betreft, verklaart het Hof in punt 147 van zijn arrest van 6 oktober 2020 dat:
<i>« l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire. »</i>	<i>« Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt ».</i>
La délimitation d'une telle mesure pourrait par exemple être fondée en fonction de catégories de personnes ou sur un critère géographique.	De afbakening van een dergelijke maatregel kan bijvoorbeeld gebaseerd zijn op categorieën van personen of op een geografisch criterium.
L'article 39quinquies diffère d'une telle réglementation de conservation ciblée de données en ce que l'ordre de conservation du procureur du Roi interviendra en principe à titre réactif et de manière circonscrite.	Artikel 39quinquies verschilt van dergelijke gerichte gegevensbewaringsregelgeving in die zin dat het bevel tot bewaring van de procureur des Konings in principe reactief en specifiek zal zijn.
La conservation rapide (ou le « quick freeze ») de données est une mesure « qui doit être	De snelle bevrozing van gegevens ("quick freeze") is een maatregel "die snel genomen

<p><i>prise rapidement afin de conserver les données chez la personne même (ou la personne morale) qui les détient pour éviter qu'elles ne soient endommagées ou perdues.»</i> (Doc. Parl., N°54/1966/001, p. 26). Les données qui font l'objet de la mesure existent et sont déjà stockées.</p>	<p><i>moet worden om de gegevens in de schoot zelf van de persoon die ze onder zich houdt, te bewaren om te voorkomen dat ze beschadigd geraken of verloren gaan."</i> (Parl. Doc., nr. 54/1966/001, blz. 26). De gegevens waarop de maatregel betrekking heeft, bestaan en zijn reeds opgeslagen</p>
<p>Cette mesure de « quick freeze » pour le passé existe dans notre législation à l'article 39ter du CIC, inséré par la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales et modifié par la loi du 5 mai 2019. Il matérialise la transposition des articles 16 et 17 de la Convention de Budapest sur la criminalité informatique.</p>	<p>Deze "quick freeze"-maatregel voor het verleden bestaat in onze wetgeving in artikel 39ter W. Sv., ingevoegd bij de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische communicatie en telecommunicatie en tot oprichting van een gegevensbank stemafdrukken, en gewijzigd bij de wet van 5 mei 2019. Het behelst de omzetting van de artikelen 16 en 17 van het Verdrag van Boedapest inzake informaticacriminaliteit.</p>
<p>L'article 39quinquies diffère notamment de l'article 39ter CIC en ce que les données ne sont pas encore collectées et stockées. Dès réception de l'ordre, les opérateurs doivent conserver les données demandées qu'ils génèrent. Il s'agit ici donc plutôt d'un « quick freeze » pour le futur.</p>	<p>Artikel 39quinquies verschilt van artikel 39ter in die zin dat de gegevens nog niet verzameld en opgeslagen zijn. Vanaf de ontvangst van de vordering moeten de operatoren de gevraagde gegevens die zij genereren, bewaren. Dit is dus meer een "snelle bevrozing" voor de toekomst.</p>
<p>La Cour de Justice estime au paragraphe 163 de l'arrêt du 6 octobre 2020 que les Etats membres peuvent prévoir dans leur législation la possibilité d'enjoindre aux fournisseurs de services de communications électroniques de procéder, sous certaines conditions, à la conservation rapide des données relatives au trafic et des données de localisation. Les conditions auxquelles cette mesure doit être subordonnée sont reprises aux points 163 à 165 de l'arrêt :</p>	<p>Het Hof van Justitie overweegt in punt 163 van het arrest van 6 oktober 2020 dat de lidstaten in hun wetgeving kunnen voorzien in de mogelijkheid om van de aanbieders van elektronische-communicatiediensten te verlangen dat zij onder bepaalde voorwaarden overgaan tot de snelle bewaring van verkeers- en locatiegegevens. De voorwaarden waaraan deze maatregel moet voldoen, zijn uiteengezet in de punten 163 tot en met 165 van het arrest:</p>
<ul style="list-style-type: none"> - décision de l'autorité compétente doit être soumise à un contrôle juridictionnel effectif ; 	<ul style="list-style-type: none"> - Het besluit van de bevoegde autoriteit is onderworpen aan effectieve rechterlijke toetsing ;
<ul style="list-style-type: none"> - inscription dans la législation de la finalité pour laquelle la conservation rapide des données peut avoir lieu ; 	<ul style="list-style-type: none"> - inschrijving in de wetgeving van het doel waarvoor de snelle opslag van gegevens mag geschieden ;

<ul style="list-style-type: none"> - limitation à la seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale ; 	<ul style="list-style-type: none"> - beperkt tot de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid ;
<ul style="list-style-type: none"> - conservation des seules données de trafic et de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. Il peut s'agir de données de trafic et de localisation <i>«afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause »</i> - voir paragraphe 165. 	<ul style="list-style-type: none"> - het bewaren van alleen die verkeers- en locatiegegevens die kunnen bijdragen tot het ophelderen van het betrokken ernstige strafbare feit of de betrokken inbreuk op de nationale veiligheid. Dit kan verkeers- en locatiegegevens omvatten <i>« die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd »</i> – Zie paragraaf 165.
<ul style="list-style-type: none"> - limitation de la durée de conservation au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient. 	<ul style="list-style-type: none"> - beperking van de bewaringstermijn tot het strikt noodzakelijke, met dien verstande dat deze termijn kan worden verlengd indien de omstandigheden en het met de maatregel nagestreefde doel zulks rechtvaardigen.
<p>Selon la jurisprudence constante de la Cour, une limitation aux droits et obligations prévus dans la directive e-privacy doit être appréciée en mesurant la gravité de l'ingérence qu'elle comporte et en vérifiant que l'importance de l'objectif d'intérêt général qu'elle poursuit est en relation avec</p>	<p>Volgens vaste rechtspraak van het Hof moet een beperking van de in de e-privacyrichtlijn vastgestelde rechten en plichten worden beoordeeld door de ernst te meten van de inmenging die zij meebrengt, en door na te gaan of het belang van de doelstelling van algemeen belang die zij nastreeft, in verhouding staat tot die ernst - zie punt 131</p>

cette gravité – voir paragraphe 131 de l'arrêt du 06.10.20).	van het arrest van het Hof van Justitie in zaak C-105/99 (zie punt 131 van het arrest van 06.10.20).
Vu que l'ingérence que comporte l'obligation de conservation ciblée prévue à l'article 39quinquies est assez similaire à celle que comporte une conservation rapide pour un même objectif, il peut être considéré qu'un tel article satisfait à l'exigence de proportionnalité requise si les modalités procédurales et matérielles déterminées par la Cour pour la conservation rapide sont respectées.	Aangezien de inmenging die de verplichting tot gerichte bewaring uit hoofde van artikel 39quinquies met zich meebrengt, sterk gelijkt op die welke een snelle bewaring met hetzelfde doel meebrengt, kan een dergelijk artikel worden geacht aan het evenredigheidsvereiste te voldoen indien de door het Hof voor snelle bewaring vastgestelde voorwaarden en modaliteiten in acht worden genomen.
Or, l'article 39quinquies prévoit de telles modalités et conditions :	Artikel 39quinquies voorziet in deze voorwaarden en modaliteiten:
<ul style="list-style-type: none"> - La finalité y est spécifiquement précisée, soit la recherche et la poursuite d'infractions qui sont de nature à entraîner un emprisonnement correctionnel d'un an ou une peine plus lourde ; 	<ul style="list-style-type: none"> - Het doel wordt specifiek omschreven, namelijk het onderzoeken en vervolgen van strafbare feiten die aanleiding kunnen geven tot een correctionele gevangenisstraf van één jaar of een zwaardere straf;
<ul style="list-style-type: none"> - La durée de conservation est limitée au strict nécessaire ; 	<ul style="list-style-type: none"> - De duur van de bewaring is beperkt tot wat strikt noodzakelijk is;
<ul style="list-style-type: none"> - Les données qui peuvent faire l'objet de la mesure sont uniquement celles qui sont susceptibles d'élucider une infraction ; 	<ul style="list-style-type: none"> - De maatregel kan alleen worden toegepast op gegevens die een strafbaar feit aan het licht kunnen brengen;
<ul style="list-style-type: none"> - Comme tout acte d'enquête, la mesure est soumise à un contrôle juridictionnel effectif. 	<ul style="list-style-type: none"> - Zoals bij elk onderzoekshandeling is de maatregel onderworpen aan effectieve rechterlijke toetsing.
Art. 18	Art. 18
Par son arrêt du 22 avril 2021, la Cour Constitutionnelle a annulé la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, en ce compris l'article 9 f) qui a remplacé le §2 de l'article 88bis et l'article 9 g) qui a inséré le §3 du même article.	Bij het arrest van 22 april 2021 heeft het Grondwettelijk Hof de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van gegevens in de sector van de elektronische communicatie vernietigd, met inbegrip van artikel 9, onder f), dat § 2 van artikel 88 bis heeft vervangen, en artikel 9, onder g), dat § 3 van datzelfde artikel heeft ingevoegd.

Or, ces paragraphes renforçaient notamment les garanties au niveau de l'accès aux données de trafic et de localisation.	Deze paragrafen versterkten echter onder meer de waarborgen voor de toegang tot verkeers- en locatiegegevens.
Suite à l'annulation, il convient de réajuster l'article 88bis en conséquence et de réintroduire certaines garanties.	Na de nietigverklaring moet artikel 88bis dienovereenkomstig worden aangepast en moeten bepaalde waarborgen opnieuw worden ingevoerd.
Le point 1° de l'article 18 supprime les mots « conformément au paragraphe 2 ». Vu que le paragraphe 2 n'existe plus, ces mots n'ont plus de raison d'être.	In het 1° van artikel 18 worden de woorden "overeenkomstig paragraaf 2" geschrapt. Aangezien paragraaf 2 niet meer bestaat, zijn deze woorden niet langer relevant.
Le point 2° de l'article 18 réintègre l'ancien § 3 qui protège les données de communication des médecins et des avocats. La mesure ne peut porter sur leurs moyens de communication électronique que dans la cadre de certaines situations très spécifiques. Ce paragraphe est une reprise des articles 39bis, §9, 56bis, 88bis, §3 et 90octies CIC.	In het 2° van artikel 18 wordt de vroegere paragraaf 3, dat de communicatiegegevens van artsen en advocaten beschermt, opnieuw opgenomen. De maatregel kan alleen betrekking hebben op hun elektronische communicatiemiddelen in bepaalde zeer specifieke situaties. Deze paragraaf is een herhaling van de artikelen 39bis, §9, 56bis, 88bis, §3 en 90octies W. Sv.
CHAPITRE 5 - Modifications de la loi du 5 août 1992 sur la fonction de police	HOOFDSTUK 5 - Wijzigingen van de wet van 5 augustus 1992 op het politieambt
Art. 19	Art. 19
L'article 19 introduit un nouveau paragraphe dans l'article 42 de la loi sur la fonction de police qui régit spécifiquement l'accès par la Cellule personnes disparues de la Police Fédérale à certaines données de communication.	Artikel 19 voert een nieuwe paragraaf in bij het artikel 42 van de Wet op het politieambt over het verzamelen van gegevens met betrekking tot elektronische communicatie door de Cel Vermiste Personen van de federale politie.
Ce nouveau paragraphe reprend en grande partie la compétence déjà existante de la Cellule, prévue à l'article 126, § 2, 5° de la loi relatives aux communications électroniques, remplacé par la loi du 29 mai 2016 et annulé par la Cour Constitutionnelle.	Deze nieuwe paragraaf neemt de al bestaande bevoegdheid van de Cel voorzien in artikel 126, § 2, 5° van de wet betreffende de elektronische communicatie, vervangen door de wet van 29 mei 2016 en vernietigd door het Grondwettelijk Hof, grotendeels over.

<p>Déjà en 2016, le législateur estimait qu'il était important de permettre à la Cellule des personnes disparues de la Police Fédérale de pouvoir directement demander l'accès de certaines données aux opérateurs: « <i>Il n'est pas approprié d'obliger la cellule de disparition de la police fédérale à solliciter un réquisitoire d'un procureur du Roi ou d'un juge d'instruction pour obtenir des données conservées par l'opérateur ou le fournisseur en vertu du présent article, lorsque la disparition inquiétante n'est pas le fait d'une infraction pénale (fugue, tentative de suicide, etc.). Le paragraphe deux prévoit dès lors que l'officier de police judiciaire de la cellule disparition peut obtenir certaines données conservées de l'opérateur ou du fournisseur par l'intermédiaire d'un service de police désigné par le Roi.</i> » (Doc Parl, 54-1567/001, p. 29).</p>	<p>Reeds in 2016 heeft de wetgever geoordeeld dat het belangrijk was om de Cel Vermiste Personen van de federale politie toe te laten om aan de operatoren direct toegang te vragen tot bepaalde gegevens: "<i>Het is niet gepast om de cel Vermiste Personen van de federale politie te verplichten een requisitoir van een procureur des Konings of van een onderzoeksrechter te vragen om gegevens te krijgen die door de operator of de aanbieder worden bewaard krachtens het onderhavige artikel, wanneer de onrustwekkende verdwijning niets te maken heeft met een strafbaar feit (vlucht, poging tot zelfmoord, enz.). Paragraaf twee bepaalt daarom dat de officier van gerechtelijke politie van de cel Vermiste Personen, via de door de Koning aangewezen politiedienst, bepaalde gegevens kan krijgen die worden bewaard door de operator of de aanbieder.</i>" (Parl. St., 54-1567/001, p. 29).</p>
<p>L'article reprend les modalités et conditions d'accès aux données, qui sont déjà prévues à l'article 126, § 2, 5° de la loi relatives aux communications électroniques.</p>	<p>Het artikel bevat de modaliteiten en de voorwaarden voor de toegang tot de gegevens, zoals nu al voorzien in artikel 126, § 2, 5° van de wet betreffende de elektronische communicatie.</p>
<p>Suite aux arrêts de la CJUE du 6 octobre 2020 et de la Cour Constitutionnelle du 22/04/2021, le gouvernement a décidé d'établir les conditions matérielles et procédurales d'accès aux données dans la loi organique de la police.</p>	<p>Naar aanleiding van de arresten van het HJEU van 6 oktober 2020 en van het Grondwettelijk Hof van 22/04/2021 heeft de regering besloten de materiële en procedurele voorwaarden voor toegang tot gegevens vast te leggen in de organieke wet van de politie.</p>
<p>A l'instar des articles 46bis, 88bis, 90quater, 464/13 et 464/25 du Code d'instruction criminelle, la notion « fournisseurs » est remplacée par la définition qui se trouve dans l'arrêt Yahoo (arrêt de la Cour de cassation du 18/01/2011) : 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.</p>	<p>Naar het voorbeeld van de artikelen 46bis, 88bis, 90quater, 464/13 en 464/25 van het Wetboek van Strafvordering wordt het begrip "aanbieders" vervangen door de definitie in het Yahoo-arrest (arrest van het Hof van Cassatie van 18/01/2011): iedereen die binnen het Belgische 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 informatie te verkrijgen, te ontvangen of te verspreiden via een elektronisch-communicatienetwerk.</p>
<p>Il y est également ajouté dans un souci de clarté « <i>Est également compris le</i></p>	<p>Voor de duidelijkheid wordt ook toegevoegd: « <i>Hieronder wordt ook de verstrekker van</i></p>

<i>fournisseur d'un service de communications électroniques. »</i>	<i>een elektronische-communicatiedienst begrepen. »</i>
Les services réquisitionnés sont tenus de coopérer à la réquisition légale émise par l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, faute de quoi ils s'exposent à des poursuites sur la base de l'article 422ter Code pénal.	De opgevorderde diensten zijn verplicht hun medewerking te verlenen aan de wettelijke vordering uitgevaardigd door de officier van gerechtelijke politie van de Cel Vermiste Personen van de Federale Politie, zoniet stellen zij zich open voor vervolging op grond van artikel 422ter Strafwetboek.
CHAPITRE 6 - Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité	HOOFDSTUK 6 - Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten
Art. 20	Art. 20
La définition de la communication reprise à l'article 3, 10° est modifiée afin de répondre à la nouvelle réalité technologique et ainsi préciser que la communication « Machine-to-Machine » relève de la « communication » telle que visée dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (LRS).	De definities van communicatie in artikel 3, 10° wordt gewijzigd om te beantwoorden aan de nieuwe technologische realiteit zodat duidelijk is dat ook de "Machine-to-Machine"-communicatie valt onder hetgeen in de wet van 30 november 1998 houdende regeling van de inlichtingendiensten (WIV) bedoeld wordt met "communicatie"
A l'article 3 le terme « opérateur » est défini comme terme fourre-tout englobant ce qui est actuellement décrit comme "opérateur d'un réseau de communications électroniques" ou "fournisseur d'un service de communications électroniques". Cette modification vise à simplifier le texte.	In artikel 3 wordt ook het begrip "operator" gedefinieerd als zijnde het containerbegrip voor hetgeen actueel als "operator van een elektronisch communicatienetwerk" of de "verstrekker van een elektronische communicatiedienst" omschreven wordt.
Art. 21	Art. 21
Premièrement, les mots « chargée de la sécurité nationale » sont ajoutés à l'article 7. Cette adaptation ne modifie pas la substance des tâches du service de renseignement et de sécurité, mais vise à préciser que les missions de renseignement et de sécurité de la Sûreté de l'Etat sont	De woorden "belast met de nationale veiligheid" worden toegevoegd aan artikel 7. Deze aanpassing brengt geen inhoudelijke wijziging aan de opdrachten van de inlichtingen- en veiligheidsdienst met zich mee maar beoogt enkel een verduidelijking dat de inlichtingen- en veiligheidsopdrachten

exécutées en vue de sauvegarder la sécurité nationale.	van de Veiligheid van de Staat plaatsvinden met het oog op de vrijwaring van de nationale veiligheid.
Art. 22	Art. 22
Les mots « chargé de la sécurité nationale » sont ajoutés à l'article 11 définissant les missions du Service Général du Renseignement. Cela ne modifie pas la substance des missions du SGRS mais vise uniquement à préciser que ces missions se situent toutes dans le cadre de la sécurité nationale.	De woorden "ter vrijwaring van de nationale veiligheid" worden toegevoegd aan artikel 11 dat de opdrachten van de Algemene Dienst Inlichting en Veiligheid bepaalt. Deze aanpassing brengt geen substantiële wijziging aan de opdrachten van de ADIV met zich mee maar beoogt enkel een verduidelijking dat deze opdrachten zich situeren binnen het kader van de nationale veiligheid.
Art. 23	Art. 23
Cette modification à l'article 16/2 découle du remplacement des mots « d'un opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques » par le mot « d'un opérateur ».	Deze wijziging aan artikel 16/2 is het gevolg van de vervanging van de woorden "operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" door het woord "operator".
Art. 24	Art. 24
L'introduction d'un nouvel article 16/2/1 fait suite à l'arrêt de la Cour de justice européenne du 6 octobre 2020, selon lequel une conservation générale et indifférenciée de données relatives au trafic et à la localisation des communications électroniques est contraire au droit européen (et notamment au droit à la vie privée). La modification de la loi vise à atteindre un meilleur équilibre entre le droit du citoyen à la vie privée, d'une part, et le devoir du gouvernement de garantir la sécurité nationale, d'autre part.	De invoering van een nieuw artikel 16/2/1 is het gevolg van de uitspraak van het Europees Hof van Justitie van 6 oktober 2020, dat stelt dat een algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens van elektronische communicatie strijdig is met EU-recht (o.a. het recht op privacy). De wetswijziging beoogt een beter evenwicht tussen het recht op privacy van de burger enerzijds, en de plicht van de overheid om de nationale veiligheid te garanderen, anderzijds.

Dans son arrêt, la Cour mentionne un certain nombre de possibilités de conservation différenciée des données.	In zijn arrest geeft het Hof een aantal mogelijkheden voor een gedifferentieerde dataretentie.
Premièrement, le dénommé « quick freeze », qui permet à un service de renseignement d'ordonner une conservation rapide de données relatives à une cible déterminée lorsque cela s'impose pour protéger la sécurité nationale.	Vooreerst is er de zogenaamde "quick freeze" waarbij een inlichtingendienst een snelle bewaring kan bevelen van de gegevens over een bepaalde target wanneer dat noodzakelijk is voor de bescherming van de nationale veiligheid.
La Cour autorise également une conservation ciblée (« targeted ») de certaines catégories de données. Ces catégories sont définies sur la base d'éléments objectifs et non discriminatoires. Les données ainsi collectées ne peuvent être conservées plus longtemps que ce qui est strictement nécessaire.	Daarnaast laat het Hof ook een gerichte ("targeted") bewaring van bepaalde categorieën van gegevens toe. Deze categorieën worden bepaald op basis van objectieve en niet-discriminatoire elementen. Hierbij mogen de gegevens niet langer bewaard worden dan strikt noodzakelijk is.
Ces « windows of opportunity » (fenêtres d'opportunité) proposées par la Cour pour une obligation différenciée de conservation des données sont concrétisées dans un nouvel article 16/2/1.	Deze "windows of opportunity" die het Hof aanreikt voor een gedifferentieerde bewaarplicht, worden geconcretiseerd in een nieuw artikel 16/2/1.
La nouvelle méthode de renseignement comporte deux possibilités :	De nieuwe inlichtingenmethode behelst twee mogelijkheden:
1° la réquisition de conservation des données de trafic et de localisation déjà générées (« quick freeze »). Dans ce cas, l'opérateur est tenu de conserver les données qu'il possède déjà au moment de la réquisition. Il s'agit en l'espèce des données conservées pour des raisons techniques, ainsi qu'à des fins de facturation, de marketing, de lutte contre la fraude, de sécurité des réseaux, etc. Ces données ne sont normalement conservées que le temps nécessaire à leurs propres finalités. Cela peut varier de quelques minutes (dans le cas de données techniques volatiles) à plusieurs années (afin pouvoir contester une facture, par exemple). Dans l'intérêt des missions de renseignement, un opérateur peut être requis de « figer » et de conserver ces données (pour une durée maximale de 6 mois, prolongeable). Cette méthode présente au moins l'avantage de sécuriser les données historiques disponibles.	1° de vordering tot bewaring van reeds gegenereerde verkeers- en lokalisatiegegevens ("quick freeze"). Met deze vordering wordt de operator bevolen gegevens te bewaren die hij sowieso in zijn bezit heeft op het moment van de vordering. Het gaat hier om gegevens die bijgehouden worden om technische redenen, maar ook om redenen van facturatie, marketing, strijd tegen fraude, voor de beveiliging van het netwerk, e.a.. Deze gegevens worden normaal gezien slechts bijgehouden zolang nodig voor de eigen doeleinden. Dit kan variëren van enkele minuten (in geval van vluchtige technische gegevens) tot meerdere jaren (bijvoorbeeld om een factuur te kunnen betwisten). In het belang van de inlichtingenopdrachten, kan een operator gevorderd worden om deze gegevens te "parkeren" en bij te houden (maximum 6 maanden, met de mogelijkheid tot verlenging). Met deze methode worden dus tenminste de beschikbare historische gegevens veiliggesteld.

Les données historiques sont indispensables dans le cadre d'une enquête de renseignement. Elles permettent de vérifier qui a contacté qui, par quel moyen, à quel moment et où ce contact a eu lieu. Jusqu'à l'arrêt de la Cour européenne, les services concernés n'avaient pas à s'inquiéter de la disponibilité de ces données puisque tout était conservé pendant 12 mois. La méthode spécifique de renseignement mentionnée à l'article 18/8 LRS permettait au service de renseignement concerné d'accéder aux données importantes pour l'enquête.	Historische gegevens zijn cruciaal in een inlichtingenonderzoek om na te gaan wie contact had met wie, met welk middel, op welk moment en waar dat contact plaatsvond. Tot de uitspraak van het Europees Hof hoefden de betrokken diensten zich geen zorgen te maken over de beschikbaarheid van deze gegevens, aangezien alles voor 12 maand werd bijgehouden. Via de specifieke inlichtingenmethode overeenkomstig artikel 18/8 WIV kon de betrokken inlichtingendienst toegang nemen tot de gegevens die van belang waren voor het onderzoek.
En raison de la jurisprudence européenne, les résultats dépendront de l'ensemble des données détenues par l'opérateur pour ses propres finalités.	Als gevolg van de Europese rechtspraak, zullen de resultaten afhankelijk zijn van de dataset die de operator voor eigen doeleinden bezit.
2° la réquisition de conservation des données de trafic et de localisation générées à dater de la réception de la réquisition (conservation des données futures). Dès qu'une personne, un outil de communication, etc. apparaît sur le radar d'un service de renseignement, l'opérateur peut être requis de conserver les données de trafic et de localisation y relatives pour une durée maximale de 6 mois (renouvelable). Le recours à la méthode spécifique de recueil de données 18/08 LRS permet, comme toujours, d'accéder à ces données.	2° de vordering tot bewaring van verkeers- en lokalisatiegegevens die gegenereerd worden vanaf de ontvangst van de vordering (bewaring van toekomstige gegevens). Zodra een persoon, een communicatiemiddel e.d. op de radar van een inlichtingendienst verschijnt, kan de operator bevolen worden om de verkeers- en lokalisatiegegevens ervan voor maximum 6 maanden (verlengbaar) te bewaren. De toegang tot deze gegevens blijft als vanouds via de specifieke BIM-methode 18/8 WIV.
La réquisition adressée à l'opérateur doit indiquer clairement quelles données de trafic et de localisation doivent être conservées (conservation des données ciblée et différenciée).	De vordering aan de operator moet duidelijk aangeven welke verkeers- en lokalisatiegegevens moeten bewaard worden (gerichte en gedifferentieerde dataretentie).
Ces éléments sont des données d'identification (nom, adresse...), des caractéristiques techniques (numéro d'appel, IMSI, IMEI...), une localisation précise (emplacement de l'antenne, coordonnées...) ou le mode d'utilisation détaillé d'un moyen (carte SIM prépayée dans un certain type de GSM qui n'est utilisé qu'une fois par semaine dans une région).	Deze elementen zijn identificatiegegevens (naam, adres, ...), technische kenmerken (oproepnummer, IMSI, IMEI, ...), een precieze locatie (antennelocatie, coördinaten, etc) of de gedetailleerde gebruikswijze van een middel (prepaid sim in een bepaald type gsm dat in een regio slechts 1 keer per week wordt aangezet).
S'il venait à être informé par un correspondant national ou étranger de	Wanneer de dienst wordt ingelicht door een binnen- of buitenlandse correspondent over

l'existence d'une personne A employée à l'aéroport et potentiellement impliquée dans les préparatifs d'un attentat à cet endroit, le service établirait les réquisitions de conservation suivantes :	een persoon A die werkt op de luchthaven en die betrokken zou zijn bij voorbereidingen van een aanslag op de luchthaven, dan zou de dienst volgende vorderingen tot bewaring opmaken:
- conservation des données de trafic et de localisation de la personne A,	- bewaring van verkeers- en lokalisatiegegevens van persoon A;
- conservation des données de trafic et de localisation du site de l'aéroport de Zaventem.	- bewaring van verkeers- en lokalisatiegegevens van de locatie Zaventem-luchthaven.
Au cours de l'enquête, il est possible que des personnes ou des moyens apparaissent, légitimant la conservation des données de trafic et de localisation y relatives, et, par voie de conséquence, l'envoi de réquisitions de conservation à cette fin.	In de loop van het onderzoek kunnen er dan nog personen of middelen opduiken waarvan de bewaring van de verkeers- en lokalisatiegegevens gewettigd is, en waarvoor er dan ook vorderingen tot bewaring zullen worden verstuurd.
Un service de renseignement peut également demander à un opérateur la conservation de données d'un groupe déterminé de personnes. Par exemple, une liste de numéros d'appel de personnes connues dans les milieux religieux radicaux pourrait faire l'objet d'une réquisition de conservation renouvelée tous les 6 mois, tant que les personnes concernées représentent une menace pour les intérêts de l'État.	Een inlichtingendienst kan ook vragen dat een operator de gegevens van een bepaalde groep van personen bijhoudt. Een lijst van de oproepnummers van gekende personen in de radicaal-religieuze scene zou bijvoorbeeld het onderwerp kunnen vormen van een vordering tot bewaring die elke 6 maand wordt verlengd, zolang de betrokkenen een bedreiging vormen voor de belangen van de staat.
Lorsque le service ne dispose que d'informations relatives à une utilisation particulière de moyens de communication, cela peut également donner lieu à une réquisition de conservation des données. Dans l'affaire Encrochat, par exemple, les utilisateurs de ce service de messagerie chiffrée actif dans la sphère criminelle ont pu être identifiés à l'aide d'une combinaison entre le type d'appareil (code TAC, qui représente une partie du code IMEI unique répertoriant le type d'appareil et le numéro de série), la carte SIM (certaines cartes SIM néerlandaises) et l'utilisation du moyen de communication (uniquement data, impossibilité de recevoir/envoyer des SMS). Des modèles d'utilisation similaires peuvent être observés lors des enquêtes d'espionnage lors desquelles des « burner phones » peuvent être détectés grâce à une combinaison de caractéristiques techniques, géographiques et temporelles (pour contacter des sources clandestines).	Ook wanneer de dienst enkel beschikt over informatie over het bijzondere gebruik van communicatiemiddelen, kan dit leiden tot een vordering tot het bewaren van gegevens. In de Encrochat-zaak, bijvoorbeeld, konden de gebruikers van deze versleutelde berichtendienst in de criminele sfeer worden opgelijst aan de hand van een combinatie van toesteltype (de TAC-code, een onderdeel van de unieke IMEI die het toesteltype en serienummer aangeeft), de simkaart (bepaalde Nederlandse simkaarten) en het type gebruik van het communicatiemiddel (enkel datagebruik, geen in- of uitgaande SMS mogelijk). Gelijkaardige gebruikspatronen zijn op te merken bij spionageonderzoeken waar "burner phones" op te sporen zijn via een combinatie van technische, geografische en temporele kenmerken (voor de contactname met clandestiene bronnen).

Les services de renseignement peuvent ensuite demander ces données conformément à l'article 18/8 LRS, de façon dûment motivée et conformément à la procédure requise pour la mise en œuvre de cette méthode spécifique de recueil de données.	De inlichtingendiensten kunnen deze gegevens vervolgens opvragen overeenkomstig artikel 18/8 WIV, met inachtnaam van de afdoende motivatie en de procedure vereist voor de inzet van deze specifieke BIM-methode.
Par analogie avec les réquisitions d'identification de l'utilisateur d'un moyen de communication (article 16/2 de la LRS), les services de renseignement ont l'obligation de tenir à jour un registre de l'ensemble des réquisitions de conservation des données de trafic et de localisation. Ce registre est transmis mensuellement pour contrôle au Comité R qui peut mettre fin immédiatement à la méthode en cas d'illégalité.	Naar analogie met de vorderingen tot identificatie van de gebruiker van een communicatiemiddel (artikel 16/2 WIV), moeten de inlichtingendiensten ook een register bijhouden van alle vorderingen tot bewaring van verkeers- en lokalisatiegegevens. Dit register wordt maandelijks ter controle overgemaakt aan het Comité I dat, in geval van onwettigheid, de methode onmiddellijk kan stopzetten.
S'il est mis fin à la méthode, le service de renseignement et de sécurité concerné en informe immédiatement l'opérateur afin que la conservation des données prenne fin.	Indien de methode wordt stopgezet, informeert de betrokken inlichten- en veiligheidsdienst hiervan onverwijld de operator opdat de bewaring van gegevens beëindigd wordt.
Afin d'éviter que des données soient conservées par l'opérateur plus longtemps que nécessaire, un délai d' 1 ans après la réquisition est prévu, dans lequel les données peuvent être demandées (conformément à l'article 18/8 LRS) par le service concerné. A l'expiration de ce délai, l'opérateur détruit les données conservées.	Om te vermijden dat gegevens niet langer dan nodig worden opgeslagen bij de operator, wordt een termijn van 1 jaar voorzien na de vordering waarin de gegevens kunnen worden opgevraagd (overeenkomstig artikel 18/8 WIV) door de betrokken dienst. Na het aflopen van deze termijn, vernietigt de operator de opgeslagen gegevens.
Art. 25	Art. 25
Une nouvelle méthode exceptionnelle étant ajoutée à l'article 18/17/1, il convient d'y faire référence à l'article 18/2, paragraphe 2.	Aangezien een nieuwe uitzonderlijke methode wordt toegevoegd aan artikel 18/17/1, dient daarnaar verwezen te worden in artikel 18/2 paragraaf 2.
Art. 26	Art. 26

Pour la suppression de l'art. 18/3, §2, 12°, il est renvoyé au commentaire consacré au remplacement de l'art. 18/8.	Voor de schrapping van art. 18/3, 12°, wordt verwezen naar de toelichting bij de wijziging van art. 18/8.
Art. 27	Art. 27
La formulation de l'article 18/7 est alignée sur la formulation des autres méthodes de renseignement.	De bewoording van artikel 18/7 wordt in lijn gebracht met de formulering van de andere inlichtingenmethoden.
Les termes « l'opérateur d'un réseau de communications ou le fournisseur d'un service de communications électroniques » sont adaptés à la nouvelle définition prévue à l'article 3, 11°.	De woorden "operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" worden aangepast aan de nieuwe definitie in artikel 3, 11°
Par ailleurs, il est ajouté à l'article 18/7 que les services de renseignement peuvent également demander les factures relatives à un abonnement spécifique. Ces factures sont susceptibles de fournir des informations intéressantes, par exemple au sujet de la personne qui effectue le paiement, des moyens de communication qui y figurent, etc.	In artikel 18/7 wordt eveneens ingevoegd dat de inlichtingendiensten ook de facturen met betrekking tot een welbepaald abonnement kunnen opgevraagd worden. Deze facturen kunnen interessante informatie opleveren bijvoorbeeld over wie de betaling verricht, welke communicatiemiddelen op de factuur staan ed.
Cette possibilité existait avant la modification de l'article 18/7 par la loi du 5 février 2016 et avait disparu lors de cette modification. Elle est dès lors réinsérée.	Deze mogelijkheid bestond voor de wijziging van artikel 18/7 door de wet van 5 februari 2016, maar werd geschrapt door voornoemde wijziging. Daarom is het opnieuw ingevoerd.
Art. 28	Art. 28
Dans son arrêt du 22 avril 2021, la Cour constitutionnelle a décidé d'annuler les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.	Bij arrest van 22 april 2021 heeft het Grondwettelijk Hof beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen.
Elle justifie l'annulation de l'ensemble de ces dispositions par le fait qu'elles sont indissociablement liées à l'obligation de conservation générale et indifférenciée des données relatives aux communications	Het Hof verantwoordt de vernietiging van het geheel van deze bepalingen door het feit dat deze onlosmakelijk verbonden zijn met de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot

électroniques par les opérateurs (voir points B.18 et B.20), principe considéré comme disproportionnel par la Cour de justice de l'Union européenne dans ses arrêts du 6 octobre 2020.	elektronische communicatie door de operatoren (zie punten B.18 en B.20), hetgeen door het Hof van Justitie van de Europese Unie als disproportioneel werd bevonden in haar arresten van 6 oktober 2020.
L'article 14 de cette loi du 29 mai 2016 modifiait l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet article 18/8 porte sur l'accès aux données de communications électroniques par les services de renseignement et de sécurité et non sur la conservation de ces données. Seul le paragraphe 2 de cet article fait référence à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.	Artikel 14 van deze wet van 29 mei 2016 wijzigde artikel 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Dit artikel 18/8 betreft de toegang tot de gegevens met betrekking tot elektronische communicatie door de inlichtingen- en veiligheidsdiensten en niet de bewaring van deze gegevens. Enkel in paragraaf 2 van dit artikel werd gerefereerd naar artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.
Dès lors, seule l'annulation de ce paragraphe se justifie eu égard aux arrêts précités.	Bijgevolg dringt zich enkel de vernietiging van deze paragraaf op in het licht van voormelde arresten.
Les autres modifications visées à l'article 14 doivent donc être réintégrées.	De overige wijzigingen doorgevoerd door artikel 14 dienen bijgevolg opnieuw geïntegreerd te worden.
L'article 18/8 ayant encore été modifié après la loi du 29 mai 2016, il est difficile de restituer la version en vigueur suite à l'annulation effectuée par la Cour. Les auteurs du projet ont donc décidé, par sécurité juridique, de remplacer entièrement l'article 18/8.	Gezien artikel 18/8 na de wet van 29 mei 2016 nogmaals werd gewijzigd, is het moeilijk om de versie van kracht ten gevolge van de vernietiging door het Hof te herstellen. De auteurs van het ontwerp hebben bijgevolg ervoor geopteerd om het volledige artikel 18/8 te vervangen omwille van redenen van rechtszekerheid.
Néanmoins, il convient de préciser qu'aucune modification n'est apportée à l'accès par les services de renseignement et de sécurité aux données de communications électroniques, ni à ses modalités.	Het is echter aangewezen om te preciseren dat geen enkele wijziging werd aangebracht aan de toegang tot de gegevens met betrekking tot de elektronische communicatie door de inlichtingen- en veiligheidsdiensten, noch aan de modaliteiten ervan.
Les deux seules modifications portent sur la 'disparation' du paragraphe 2 logiquement annulé par la Cour constitutionnelle et sur le remplacement de la notion de « opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique » par le mot « opérateur » suite à la nouvelle définition	De enige twee wijzigingen betreffen de "verdwijning" van paragraaf 2, die logischerwijze werd vernietigd door het Grondwettelijk Hof en de vervanging van het begrip "operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst" door het woord "operator" ten gevolge van

insérée à l'article 3, 10°/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité	de nieuwe definitie die werd ingevoegd in artikel 3, 10°/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten
L'accès aux données par les services de renseignement et de sécurité visé à l'article 18/8 porte bien entendu sur toutes les données conservées par les opérateurs, peu importe pour quelle finalité.	De toegang tot de gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in artikel 18/8, heeft betrekking op alle gegevens bewaard door de operatoren, ongeacht de doelstelling.
En effet, comme le précise la Cour de Justice de l'Union européenne dans son arrêt du 6 octobre 2020, en ses points 166 et 167, un accès à des données conservées pour un objectif de lutte contre la criminalité ou pour les besoins propres des opérateurs (facturation, marketing, sécurité des réseaux, ...) est a fortiori justifié par l'objectif de sauvegarde de la sécurité nationale.	Zoals het Hof van Justitie van de Europese Unie in zijn arrest van 6 oktober 2020 in de punten 166 en 167 heeft verklaard, is de toegang tot de gegevens die zijn bewaard met het oog op de bestrijding van criminaliteit of voor de eigen behoeften van de operatoren (facturatie, marketing, netwerkbeveiliging, enz.) a fortiori gerechtvaardigd ter vrijwaring van de nationale veiligheid.
Art. 29	Art. 29
Une nouvelle méthode exceptionnelle étant ajoutée à l'article 18/17/1, il convient d'y faire référence à l'article 18/10, §4, alinéa 4.	Aangezien een nieuwe uitzonderlijke methode wordt toegevoegd aan artikel 18/17/1, dient daarnaar verwezen te worden in artikel 18/10, §4, vierde lid.
Art. 30	Art. 30
Cette modification de l'article 18/17 (réquisition d'interception de communications) découle du remplacement des mots « d'un opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques » par le mot « d'un opérateur ».	Deze wijziging aan artikel 18/17 (vordering voor een interceptie van communicatie) is het gevolg van de vervanging van de woorden "operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" door het woord "operator".
Art. 31	Art. 31

<p>Dans son arrêt du 6 octobre 2020, la Cour de Justice précise que, dans des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le concours des opérateurs peut être requis pour procéder à la conservation généralisée et indifférenciée des données de télécommunication. La condition connexe prévoit que les données ne seront pas conservées plus longtemps que le stricte nécessaire et que la réquisition fait l'objet d'un contrôle effectif, soit par un tribunal, soit par un organe administratif indépendant. Conformément à cette jurisprudence, une telle réquisition de conservation généralisée est insérée en tant que nouvelle méthode exceptionnelle de renseignement.</p>	<p>In zijn arrest van 6 oktober 2020 stelt het Hof van Justitie dat in situaties waarbij de lidstaat wordt geconfronteerd met een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is, er een bevel kan worden opgelegd aan operatoren om telecommunicatiegegevens algemeen en ongedifferentieerd te bewaren. Als voorwaarde hiervoor geldt dat de gegevens niet langer bewaard worden dan strikt noodzakelijk is en het bevel het voorwerp uitmaakt van een effectieve controle, hetzij door een rechtbank, hetzij door een onafhankelijk administratief orgaan. In lijn met deze rechtspraak wordt dergelijk bevel tot algemene bewaring, ingevoegd als een nieuwe, uitzonderlijke inlichtingenmethode.</p>
<p>Une méthode exceptionnelle de renseignement ne peut être autorisée qu'en cas de menace très grave pour la sécurité de l'État et après avis conforme de la Commission BIM (organe administratif indépendant). Cette Commission évalue non seulement la légalité de la méthode, mais également la proportionnalité et la subsidiarité. En outre, par le biais d'une procédure d'extrême urgence, la Commission peut intervenir très rapidement, tout en conservant sa fonction de contrôle, ce qui est nécessaire dans le cas d'une menace grave réelle et actuelle. Une fois la méthode approuvée, le Comité permanent R peut également exercer sa compétence de contrôle.</p>	<p>Een uitzonderlijke inlichtingenmethode kan slechts gemachtigd worden ingeval van een zeer ernstige bedreiging van de veiligheid van de staat en na eensluitend advies van de BIM-commissie (onafhankelijk administratief orgaan). Deze commissie beoordeelt niet alleen de wettelijkheid van de methode, maar ook de proportionaliteit en de subsidiariteit. Via een hoogdringendheidsprocedure kan de Commissie bovendien zeer snel optreden, zonder aan haar controlefunctie in te boeten, hetgeen noodzakelijk is in geval van een reële en actuele ernstige bedreiging. Eens de methode is goedgekeurd, kan ook het Vast Comité I zijn toezichtsbevoegdheid uitoefenen.</p>
<p>Il est indiqué que la réquisition envoyée à l'opérateur mentionne la nature de l'avis conforme. Cette formulation peut paraître un peu étrange mais étant utilisée dans d'autres articles de la loi, le choix a été fait de garder une certaine harmonisation. L'objectif visé par cette formulation est que l'opérateur soit informé de l'existence d'un avis conforme (c'est-à-dire un accord) de la Commission, sans lequel une conservation indifférenciée ne peut pas avoir lieu.</p>	<p>De tekst voorziet dat het aan de operator gerichte verzoek de aard van het eensluitend advies moet vermelden. Deze formulering kan enigszins vreemd overkomen, maar omdat zij ook in andere delen van de wet wordt gebruikt, werd gekozen voor een zekere harmonisatie. Het doel van deze formulering is ervoor te zorgen dat de operator op de hoogte is van het bestaan van een eensluitend advies (namelijk een akkoord) van de Commissie, zonder dewelke er geen ongedifferentieerde bewaring kan plaatsvinden.</p>
<p>L'autorisation prise par le dirigeant du service concerné de mettre en œuvre cette</p>	<p>De machtiging van het betrokken diensthoofd om deze uitzonderlijke methode</p>

méthode exceptionnelle est transmise au ministre compétent pour information.	toe te passen, wordt ter informatie aan de bevoegde minister overgemaakt.
Il convient de préciser que le but est donc d'informer le ministre compétent qu'une conservation indifférenciée est déclenchée. Cela n'est pas à confondre avec l'autorisation qui pourrait éventuellement être prise par le ministre compétent, en application de l'article 18/10, §3, alinéa 3, si la commission ne rend pas son avis dans les quatre jours ou est dans l'impossibilité de délibérer dans ce délai.	Het doel is de bevoegde minister in kennis te stellen van het feit dat een ongedifferentieerde bewaring gestart is. Dit mag niet worden verward met de toelating die eventueel door de bevoegde minister zou kunnen worden verleend met toepassing van artikel 18/10, §3, derde lid, wanneer de commissie niet binnen de vier dagen advies uitbrengt of niet in staat is binnen deze termijn te beraadslagen.
Dans le cas où une situation similaire à celle du 13 novembre 2015, le soir des attentats de Paris, venait à se produire, et dès lors que l'importante sévérité de la menace pour la Belgique ne ferait plus aucun doute, la conservation généralisée et indifférenciée pour le territoire du Royaume s'imposerait par le recours à cette méthode exceptionnelle. Les services de renseignement seraient ainsi en mesure d'utiliser immédiatement la méthode spécifique pour demander des données de trafic et de localisation (article 18/8) concernant les personnes et les moyens apparaissant dans les enquêtes relatives à cette menace très grave.	In geval een soortgelijke situatie zich zou voordoen als op 13 november 2015, de avond van de aanslagen in Parijs, dan zou zodra de zeer ernstige dreiging naar België duidelijk wordt, via deze uitzonderlijk methode de algemene en ongedifferentieerde bewaring worden afgedwongen voor het grondgebied van het Rijk. Dat laat toe dat de inlichtingendiensten onmiddellijk gebruik kunnen maken van de specifieke methode voor het opvragen van verkeers- en lokalisatiegegevens (artikel 18/8) voor die personen en middelen die opduiken in de onderzoeken naar deze zeer ernstige bedreiging.
La période de conservation est limitée à six mois et peut être renouvelée. Tous les deux mois, le service de renseignement fournit à la Commission un état de la situation. Si plus aucune conservation généralisée n'est nécessaire dans l'intérêt de l'exercice de la mission de renseignement, il est mis fin immédiatement à la méthode, et la conservation généralisée et indifférenciée prend dès lors fin.	De bewaarperiode wordt beperkt tot zes maanden die kan verlengd worden. Om de twee maanden geeft de inlichtingendienst een stand van zaken aan de commissie. Indien er geen algemene bewaring meer nodig is ten behoeve van de inlichtingenopdracht, wordt de methode onmiddellijk beëindigt en eindigt dus de algemene en ongedifferentieerde bewaring.
CHAPITRE 7 - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	HOOFDSTUK 7 - Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
Art. 32	Art. 32

<p>Conformément aux articles 82, 2°, et 84 actuels de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, l'auditeur de la FSMA peut, moyennant l'autorisation préalable d'un juge d'instruction, requérir la communication des données de trafic et de localisation de communications électroniques et demander les détails de paiement des services de communications électroniques. Le présent projet vise à modifier l'article 84 de cette loi en instaurant, à certaines conditions, la possibilité pour l'auditeur de la FSMA d'ordonner, sans l'autorisation préalable d'un juge d'instruction, aux opérateurs d'un réseau de communications électroniques et à toute personne qui met à disposition ou offre, sur le territoire belge, 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 (appelés ci-après "les opérateurs"), de conserver ces données temporairement (et de procéder ainsi à ce que l'on appellera ci-dessous un "quick freeze").</p>	<p>Overeenkomstig de bestaande artikelen 82, 2° en 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, kan de auditeur van de FSMA, mits voorafgaande toestemming van een onderzoeksrechter, de mededeling vorderen van verkeers- en locatiegegevens van elektronische communicatie en van betalingsdetails van elektronische communicatiediensten. In artikel 84 van deze wet wordt thans onder bepaalde voorwaarden de mogelijkheid ingevoerd voor de auditeur van de FSMA om, zonder de voorafgaande toestemming van een onderzoeksrechter, aan de operatoren van een elektronisch communicatienetwerk en iedereen die binnen het Belgisch grondgebied 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 elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden (hierna "de operatoren" genoemd), te bevelen deze gegevens tijdelijk te bewaren (hierna "quick freeze" genoemd).</p>
<p>Il s'agit d'un "quick freeze" tel qu'autorisé à certaines conditions par l'arrêt Quadrature de la Cour de justice de l'Union européenne rendu le 6 octobre 2020, mais avec une portée très limitée : il porte uniquement sur des données existantes qui, au moment où est émis l'ordre, sont encore conservées mais risquent d'être supprimées ou rendues anonymes le temps d'obtenir l'autorisation du juge d'instruction pour requérir ces données. Dans la mesure où l'auditeur de la FSMA ne peut requérir ces données que moyennant l'autorisation préalable du juge d'instruction, il s'écoule en effet toujours un laps de temps entre le moment où l'auditeur souhaite requérir les données et la demande proprement dite des données avec l'autorisation du juge d'instruction. Pour éviter que les données ne soient entre-temps plus disponibles, l'auditeur de la FSMA peut adresser aux opérateurs un ordre de quick freeze leur enjoignant de conserver ces données, le cas échéant, plus longtemps que durant les délais maximaux</p>	<p>Het betreft een "quick freeze" zoals onder bepaalde voorwaarden toegelaten door het arrest Quadrature van het Europees Hof van Justitie van 6 oktober 2020, maar met een zeer beperkte draagwijdte: zijnde enkel bestaande gegevens, die op het moment van dit bevel nog bewaard worden maar riskeren te worden verwijderd of anoniem gemaakt in afwachting van de toestemming van de onderzoeksrechter om deze gegevens op te vragen. Omdat de auditeur van de FSMA deze gegevens enkel kan opvragen met voorafgaande toestemming van de onderzoeksrechter, verstrijkt er immers steeds een periode tussen het moment waarop de auditeur de gegevens wenst op te vragen en de eigenlijke opvraging van de gegevens met toestemming van de onderzoeksrechter. Om te vermijden dat de gegevens intussen niet meer beschikbaar zijn, kan de auditeur van de FSMA met een bevel tot quick freeze aan de operatoren bevelen dat zij deze gegevens desgevallend langer bewaren dan</p>

<p>fixés par la loi du 13 juin 2005 relative aux communications électroniques (laquelle prévoit, plus précisément dans ses nouveaux articles 122, § 4/2, et 123, § 1^{er}, 5°, une dérogation concernant les données qui sont nécessaires pour répondre à une obligation légale dans le chef des opérateurs, telle qu'un quick freeze ordonné par l'auditeur de la FSMA).</p>	<p>de maximale termijnen voorzien in de wet van 13 juni 2005 betreffende de elektronische communicatie (die hierop, met name in het nieuwe artikel 122, § 4/2 en artikel 123, § 1, 5°, een afwijking bepalen voor de gegevens die noodzakelijk zijn om gevolg te geven aan een wettelijke verplichting in hoofde van de operatoren, waaronder ook een quick freeze op bevel van de auditeur van de FSMA begrepen wordt).</p>
<p>Cette possibilité de quick freeze n'est en outre prévue que pour les violations de l'interdiction d'abus de marché (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)), qui constituent une infraction grave. Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet important. Il s'agit, au sein du secteur financier, de l'une des infractions les plus graves, comme en témoignent notamment le fait que le règlement relatif aux abus de marché exige pour ces infractions des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières européennes, ainsi que le fait que la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché impose aux Etats membres de prévoir également des sanctions pénales pour les abus de marché (disposition transposée dans les articles 39 et 40 de la loi du 2 août 2002). Dans le cadre des enquêtes généralement longues et complexes qui concernent les abus de marché, les données de communications électroniques jouent souvent un rôle important dans l'administration de la preuve, par exemple pour constater que des personnes ont, à un moment donné, été en contact l'une avec l'autre et qu'il existe une relation entre deux ou plusieurs personnes.</p>	<p>Bovendien wordt deze mogelijkheid tot quick freeze enkel voorzien voor inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), wat een ernstig misdrijf uitmaakt. De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de meest ernstige inbreuken, wat o.m. blijkt uit het feit dat de Verordening marktmisbruik voor deze inbreuken aanzienlijk hogere minimale maximumboetes vereist dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere Europese financiële wetgeving, alsook uit het feit dat Richtlijn 2014/57/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende strafrechtelijke sancties voor marktmisbruik de lidstaten oplegt om voor marktmisbruik ook strafrechtelijke sancties te voorzien (uitgewerkt in de artikelen 39 en 40 van de wet van 2 augustus 2002). In het kader van de doorgaans complexe en tijdsintensieve onderzoeken inzake marktmisbruik spelen elektronische communicatiegegevens dikwijls een belangrijke rol in de bewijsvoering, bijvoorbeeld om vast te stellen dat personen op een bepaald moment met elkaar in contact zijn geweest en er tussen twee of meer personen een relatie bestaat.</p>
<p>Les garanties matérielles et procédurales nécessaires sont à cet égard prévues :</p>	<p>Ter zake worden de nodige materiële en procedurele waarborgen voorzien:</p>

<ul style="list-style-type: none"> - le quick freeze n'est possible qu'à des fins bien déterminées, à savoir en vue d'éviter, lors de la détection, l'examen et la poursuite d'abus de marché (tant par la FSMA que dans le cadre d'une demande de coopération émanant d'autorités compétentes d'autres Etats membres de l'EEE ou de pays tiers qui sont dotées de pouvoirs comparables à ceux de la FSMA), que des données de trafic et de localisation nécessaires à la manifestation de la vérité ne soient supprimées ou rendues anonymes, dans l'attente de l'obtention de l'autorisation d'un juge d'instruction pour requérir ces données ; 	<ul style="list-style-type: none"> - de quick freeze is enkel mogelijk voor welbepaalde doeleinden, met name om bij het opsporen, onderzoeken en vervolgen van marktmisbruik (zowel door de FSMA als in het kader van een verzoek tot samenwerking van bevoegde autoriteiten van andere lidstaten van de EER of van derde staten met bevoegdheden die vergelijkbaar zijn aan die van de FSMA) te vermijden dat verkeers- en locatiegegevens die noodzakelijk zijn om de waarheid aan de dag te brengen, worden verwijderd of anoniem gemaakt, in afwachting van het bekomen van de toestemming van een onderzoeksrechter om deze gegevens op te vragen;
<ul style="list-style-type: none"> - seul l'auditeur (ou, en son absence, l'auditeur adjoint) de la FSMA peut ordonner le quick freeze ; 	<ul style="list-style-type: none"> - enkel de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) van de FSMA kan de quick freeze bevelen;
<ul style="list-style-type: none"> - l'auditeur (ou, en son absence, l'auditeur adjoint) indique dans son ordre de quick freeze les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver son ordre, des principes de proportionnalité et de subsidiarité. Il doit, dans ce cadre, mentionner notamment la ou les personnes qui font l'objet de l'ordre de conservation, les catégories de données de trafic et de localisation qui doivent être conservées et la période du passé sur laquelle porte l'ordre. Il doit en outre préciser les motifs pour lesquels ces données peuvent contribuer à la mise au jour d'abus de marché et les raisons pour lesquelles elles risquent d'être supprimées ou rendues anonymes par les opérateurs de télécommunications, par exemple par suite du respect des délais de conservation limités prévus par la loi du 13 juin 2005 relative aux communications électroniques ; 	<ul style="list-style-type: none"> - de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) doet in zijn bevel tot quick freeze opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn bevel. Daarbij dient hij met name de persoon of personen waarop de bewaring betrekking heeft, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden en de periode in het verleden waarover het bevel zich uitstrekt, te vermelden. Bovendien moet hij motiveren waarom deze gegevens kunnen bijdragen tot het aan het licht brengen van marktmisbruik en waarom ze riskeren te worden verwijderd of anoniem te worden gemaakt door de telecomoperatoren, zo bijvoorbeeld als gevolg van de beperkte bewaartermijnen bepaald in de wet van 13 juni 2005 betreffende de elektronische communicatie;
<ul style="list-style-type: none"> - il s'agit d'une conservation d'une durée limitée, à savoir jusqu'à ce que l'auditeur ait reçu d'un juge d'instruction l'autorisation de requérir ces données ; 	<ul style="list-style-type: none"> - het gaat om een bewaring voor een beperkte tijd, met name totdat de auditeur de toestemming van een

	onderzoeksrechter heeft bekomen voor de opvraging van deze gegevens;
- les opérateurs doivent veiller à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée ;	- de operatoren moeten ervoor zorgen dat de integriteit van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden;
- 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 ;	- iedere persoon die uit hoofde van zijn functie 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;
- bien que l'auditeur ne soit pas tenu, pour ordonner le quick freeze, d'obtenir préalablement l'autorisation d'un juge d'instruction (contrairement à ce qui est le cas pour la demande de communication des données), un contrôle juridictionnel effectif sera toutefois bel et bien opéré (a posteriori) : le juge d'instruction amené à statuer sur la demande d'autorisation préalable qui lui est adressée par l'auditeur en vue de requérir les données, se prononcera également sur le quick freeze. S'il estime que le quick freeze n'était pas légitime ou pas justifié ou s'il refuse, pour une autre raison, de donner l'autorisation de requérir les données de trafic et de localisation qui font l'objet du quick freeze, ce quick freeze prendra fin. Notons par ailleurs que, dans le cadre d'une éventuelle procédure ultérieure, il sera également question d'un contrôle juridictionnel opéré a posteriori : dans le cas de poursuites pénales, par la chambre de mise en accusation et le juge du fond qui se prononce sur la régularité de la procédure et des actes d'investigation ; dans le cas d'une procédure de sanction administrative, par la Cour des marchés qui statue sur le recours formé contre les décisions de sanction de la FSMA et qui se prononce éventuellement aussi sur la régularité de la procédure et des actes d'investigation.	- hoewel de auditeur voor de quick freeze niet voorafgaand de toestemming van een onderzoeksrechter moet bekomen (in tegenstelling tot voor de vordering tot mededeling van de gegevens), vindt er (a posteriori) wel een effectieve rechterlijke controle plaats: de onderzoeksrechter die oordeelt over het verzoek van de auditeur tot voorafgaande toestemming om de gegevens op te vragen, zal ook oordelen over de quick freeze. Indien hij oordeelt dat de quick freeze niet wettig of niet gerechtvaardigd was of indien hij om een andere reden de toestemming weigert om de verkeers- en locatiegegevens die het voorwerp uitmaken van de quick freeze op te vragen, komt de quick freeze ten einde. Daarnaast is het zo dat er in het kader van een eventuele latere procedure ook een a posteriori rechterlijke controle zal plaatsvinden: in geval van strafvervolgning, door de kamer van inbeschuldigingstelling en de rechter ten gronde die de regelmatigheid van de procedure en de onderzoeksdaeden beoordeelt, in geval van administratieve sanctieprocedure, door het Marktenhof dat oordeelt over het beroep tegen de sanctiebeslissingen van de FSMA en dat desgevallend ook de regelmatigheid van de procedure en de onderzoeksdaeden beoordeelt.

CHAPITRE 8 - 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	HOOFDSTUK 8 - Wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten
Art. 33	Art. 33
<p>Cet article instaure une possibilité d'identification sur la base d'une adresse IP ou d'un numéro de téléphone, suite aux nouvelles dispositions introduites aux articles 127, § 1er, et 127/1, § 1er, de la loi de la loi du 13 juin 2005 relative aux communications électroniques (ci-après loi Télécom). Le commerce en ligne explose. Par conséquent, de plus en plus de particuliers et d'entreprises vendent des biens et des services en ligne. Ceci a pour conséquence que l'Inspection Produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement doit elle aussi se concentrer de plus en plus sur le contrôle de ce commerce en ligne. Afin de pouvoir exercer correctement son rôle d'autorité de surveillance du marché, elle doit disposer des instruments juridiques appropriés.</p>	<p>Dit artikel voert de mogelijkheid in om een identiteit te achterhalen op grond van het IP-adres of telefoonnummer, in navolging van de nieuwe bepalingen in artikelen 127, § 1, en 127/1, § 1, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna Telecomwet). Online handel groeit explosief. Er zijn dan ook steeds meer personen en ondernemingen die goederen en diensten online verkopen. Dit heeft als gevolg dat ook de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu zich meer en meer moet toespitst op het controleren van deze online handel. Om haar rol als markttoezichtautoriteit op een degelijke manier te kunnen uitvoeren, moet zij over de juiste juridische instrumenten beschikken.</p>
<p>Le caractère hautement anonyme qu'offre internet pour les vendeurs forme à cet égard un important défi à relever. Souvent, l'adresse IP et le numéro de téléphone sont les seules données que le service d'inspection peut obtenir grâce à la coopération de la plateforme en ligne où l'infraction a été commise. Il est donc très important que le service d'inspection puisse identifier au moyen de ces données ceux qui commettent des infractions à la mise sur le marché de produits, en demandant la mise à disposition de documents et de données d'identification à l'opérateur d'un réseau de communications électroniques et au fournisseur d'un service de communications électroniques. Il s'agit des données d'identité mentionnées à l'article 127, § 1er, de la loi</p>	<p>De grote anonimiteit die het internet biedt aan verkopers, vormt hierbij een belangrijke uitdaging. Vaak zijn het IP-adres of het telefoonnummer de enige gegevens die de inspectiedienst kan bekomen door medewerking van de online marktplaats waarop de inbreuk werd begaan. Daarom is het van groot belang dat de inspectiedienst diegenen, die inbreuken begaan bij het op de markt brengen van producten, kan identificeren aan de hand van deze gegevens, door identificatiegegevens te vorderen van de operator van een elektronisch communicatienetwerk en verstrekker van een elektronische communicatiedienst. Het gaat over de identiteitsgegevens vermeld in artikel 127, § 1, van de Telecomwet: bijv. naam,</p>

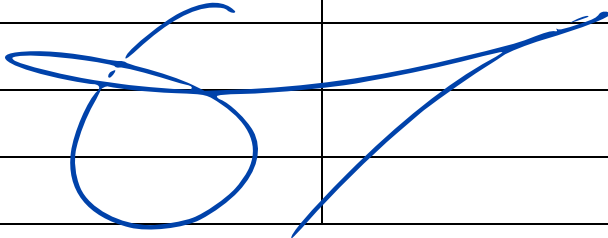
Télécom: ex. nom, prénom, date de naissance de l'abonné et/ou une copie de sa pièce d'identité (ex. passeport).	voornaam, geboortedatum en/of een kopie van zijn identiteitsstuk (bijv. paspoort).
L'autorisation accordée offre des garanties suffisantes pour assurer le respect de la vie privée des personnes : seul le numéro de téléphone ou l'adresse IP à la source d'une communication électronique sera utilisé, et pour autant que cette communication soit publique: Il peut s'agir par exemple de l'adresse IP sous laquelle un compte de vente a été créé ou une annonce de vente a été placée, ou du numéro de téléphone renseigné dans une offre en ligne. De plus, à la suite de cette autorisation, des mesures organisationnelles et techniques seront mises en œuvre au sein du SPF Santé après avoir effectué une analyse d'impact sur la protection des données (AIPD) afin d'identifier et de réduire les risques pour la vie privée liés à ce traitement des données.]	De machtiging biedt voldoende waarborgen voor het respect van het privéleven van personen: er wordt enkel het IP-adres of telefoonnummer gebruikt dat aan de bron ligt van de elektronische communicatie en voor zover deze openbaar van aard is: het gaat bijvoorbeeld over het IP adres waaronder een verkoopaccount werd aangemaakt of een verkoopadvertentie werd geplaatst of over het telefoonnummer vermeld in een online aanbieding. Bovendien worden binnen de FOD Volksgezondheid naar aanleiding van deze bevoegdheid organisatorische en technische maatregelen doorgevoerd als gevolg van een Data Protection Impact Assessment (DPIA) om privacy-risico's van deze gegevensverwerking in kaart te brengen en ze te verkleinen.]
Chaque demande d'identification doit être approuvée au préalable, par le chef du service d'inspection concerné du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement.]]	De identificatieverzoek dient voorafgaand door het hoofd van de betreffende inspectiedienst van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.
CHAPITRE 9 - Modification 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 (« loi NIS »)	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 ("NIS wet")
Art. 34	Art. 34
L'article 34 prévoit une nouvelle formulation de 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 (« loi NIS »). Les paragraphes 1er, 3 et 4 reprennent le contenu actuel des alinéas 1 à	Artikel 34 voorziet in een nieuwe formulering van 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 ("NIS-wet"). De paragrafen 1, 3 en 4 nemen de huidige

<p>4 de l'article 62. Le nouveau paragraphe 2 habilite quant à lui le CCB, en tant que CSIRT national, à obtenir l'accès à des données d'identification, de trafic et de localisation auprès des opérateurs de communications électroniques.</p>	<p>inhoud van lid 1 tot 4 van artikel 62 over. De nieuwe paragraaf 2 machtigt het CCB, als nationaal CSIRT, om toegang te krijgen tot identificatie-, verkeers- en locatiegegevens bij elektronische-communicatieoperatoren.</p>
<p>En effet, comme énoncé au commentaire de l'article 8 de la présente loi, le CSIRT national (Centre pour la Cybersécurité Belgique, ci-après le « CCB ») doit être en mesure, le cas échéant, d'obtenir des différents opérateurs, des données de communications électroniques afin d'accomplir ses missions légales. Ces dernières relèvent notamment de la prévention et de la détection des infractions en matière de cybercriminalité, de la prévention de menaces contre la sécurité publique liées à la cybersécurité ainsi que de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques.</p>	<p>Zoals vermeld in de commentaar bij artikel 8 van deze wet, moet het nationale CSIRT (Centrum voor Cybersecurity België, hierna het "CCB") in voorkomend geval immers in staat zijn om van de verschillende operatoren elektronische-communicatiegegevens te verkrijgen teneinde zijn wettelijke opdrachten te vervullen. Deze opdrachten betreffen met name het voorkomen en opsporen van misdrijven inzake cybercriminaliteit, het voorkomen van bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging en het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten.</p>
<p>Le paragraphe 2 dispose ainsi que le CSIRT national peut obtenir des opérateurs de communications électroniques les données d'identification, de trafic et de localisation conservées par ceux-ci, lorsque cela s'avère strictement nécessaire à la réalisation des tâches énumérées à l'article 60, a) à e), de la loi NIS.</p> <p>Les tâches concernées sont le suivi des incidents sur la sécurité des réseaux et des systèmes d'information, la diffusion d'informations sur les risques et incidents auprès des parties intéressées, l'intervention en cas d'incident, l'analyse dynamique des risques et incidents, ainsi que la détection, l'observation et l'analyse des problèmes de sécurité informatique.</p>	<p>Paragraaf 2 bepaalt dus dat het nationale CSIRT van elektronische-communicatieoperatoren identificatie-, verkeers- en locatiegegevens die door hen worden bewaard, kan verkrijgen, indien dat strikt noodzakelijk is voor de uitvoering van de taken opgesomd in artikel 60, a) tot e), van de NIS-wet.</p> <p>De betrokken taken zijn het monitoren van incidenten in verband met de beveiliging van netwerk- en informatiesystemen, het verspreiden van informatie over risico's en incidenten ten behoeve van de betrokken belanghebbende partijen, het reageren op incidenten, de dynamische risico- en incidentanalyse, alsook het opsporen, observeren en analyseren van computerbeveiligingsproblemen.</p>
<p>Les infractions en matière de cybercriminalité visent notamment l'accès à un système informatique sans autorisation (article 550bis du Code pénal) ; l'introduction, la modification ou la suppression de données, dans un système informatique, sans autorisation (article 550ter du Code pénal) ; la recherche, avec une intention frauduleuse, d'un avantage</p>	<p>Misdrijven inzake cybercriminaliteit hebben met name betrekking op de indringing in een informaticasysteem zonder machtiging (artikel 550<i>bis</i> van het Strafwetboek); het invoeren, wijzigen of wissen van gegevens in een informaticasysteem zonder machtiging (artikel 550<i>ter</i> van het Strafwetboek); het met bedrieglijk opzet nastreven van een economisch voordeel</p>

<p>économique au travers de l'intrusion, de la modification ou de la suppression de données dans un système informatique ou de la modification de l'utilisation normale des données dans un système informatique (article 504^{quater} du Code pénal) ; la modification ou l'effacement des données dans un système informatique, ainsi que la modification par tout moyen technologique de l'utilisation possible des données dans un système informatique et modifiant par-là la portée juridique de telles données (210^{bis} du Code pénal).</p>	<p>door gegevens in een informaticasysteem in te voeren, te wijzigen of te wissen, of door de normale aanwending van gegevens in een informaticasysteem te veranderen (artikel 504^{quater} van het Strafwetboek); het wijzigen of wissen van gegevens in een informaticasysteem, alsook het met enig technologisch middel veranderen van de mogelijke aanwending van gegevens in een informaticasysteem, waardoor de juridische draagwijdte van dergelijke gegevens verandert (210^{bis} van het Strafwetboek).</p>
<p>Ces infractions sont d'une nature particulière par rapport aux autres infractions car elles sont nécessairement commises au moyen d'un service de communications électroniques de sorte que le CCB ne peut prévenir efficacement des incidents de sécurité informatique que s'il est en mesure d'accéder à certaines données de communications électroniques. En effet, ces incidents résultent souvent d'infractions de cybercriminalité, lesquelles ne laissent que des traces digitales. Cela signifie que la seule manière de prévenir ou détecter ces infractions pénales (et les incidents de sécurité qui pourraient en résulter) est d'avoir accès aux données numériques que les infractions ont laissées.</p>	<p>Deze misdrijven onderscheiden zich van andere misdrijven omdat ze noodzakelijkerwijs gepleegd worden met behulp van een elektronische-communicatiedienst. Daardoor kan het CCB computerbeveiligingsincidenten alleen doeltreffend voorkomen indien het toegang kan hebben tot bepaalde elektronische-communicatiegegevens. Deze incidenten zijn immers vaak het gevolg van misdrijven inzake cybercriminaliteit, die alleen digitale sporen nalaten. Bijgevolg kunnen deze misdrijven (en de beveiligingsincidenten die eruit kunnen voortvloeien) alleen worden voorkomen of opgespoord door toegang te krijgen tot de digitale gegevens die bij de misdrijven zijn achtergelaten.</p>
<p>Vu l'augmentation et la fréquence des incidents en matière de cybersécurité, le CCB ne pourrait prévenir et détecter en temps utile ni les infractions en matière de cybercriminalité, ni les menaces contre la sécurité publique liées à la cybersécurité, ni les défaillances de la sécurité des réseaux s'il devait obtenir l'autorisation préalable d'une juridiction ou d'une autorité nationale indépendante pour accéder à ces données de communications électroniques.</p>	<p>Gezien de toename en frequentie van cyberbeveiligingsincidenten kan het CCB misdrijven inzake cybercriminaliteit, bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging of beveiligingsproblemen bij netwerken niet voorkomen en tijdig opsporen indien de voorafgaande toestemming van een rechterlijke instantie of onafhankelijke nationale autoriteit vereist is om toegang te krijgen tot deze elektronische-communicatiegegevens.</p>
<p>Bien entendu, le CCB demeure soumis aux contrôles juridictionnels de droit commun de l'administration, à savoir soit le contrôle des juridictions judiciaires, soit le contrôle de la section du contentieux administratif du Conseil d'Etat. Il est également soumis au contrôle de l'Autorité de protection des données.</p>	<p>Uiteraard blijft het CCB onderworpen aan de gemeenrechtelijke rechterlijke controle op het bestuur, namelijk de toetsing door gewone rechtscolleges of de toetsing door de afdeling bestuursrechtspraak van de Raad van State. Het is eveneens onderworpen aan het toezicht van de Gegevensbeschermingsautoriteit.</p>

<p>En outre, l'accès du CCB est limité à ce qui est strictement nécessaire à la réalisation des tâches visées aux points a) à e) de l'article 60 de la loi NIS. Par ailleurs, seules les données d'identification, de trafic ou de localisation conservées par les opérateurs pourraient être obtenues par le CSIRT national. Il faut également rappeler que les dispositions de la loi NIS relatives au traitement et à la protection des données à caractère personnel s'appliquent bien évidemment aux données auxquelles le CSIRT national aura accès.</p>	<p>De toegang van het CCB is bovendien beperkt tot hetgeen strikt noodzakelijk is voor de uitvoering van de taken bedoeld in punt a) tot e) van artikel 60 van de NIS-wet. Voorts zou het nationale CSIRT alleen identificatie-, verkeers- of locatiegegevens die door de operatoren worden bewaard, kunnen verkrijgen. Ook zijn de bepalingen van de NIS-wet betreffende de verwerking en bescherming van persoonsgegevens uiteraard van toepassing op de gegevens waartoe het nationale CSIRT toegang zal hebben.</p>
<p>Le paragraphe 2, alinéa 2, prévoit que les fonctionnaires dirigeants du CSIRT national désignent expressément les personnes habilitées à solliciter les données d'identification, de trafic ou de localisation auprès des opérateurs. Seules les personnes habilitées peuvent également traiter ces données. Cette disposition a pour objectif de limiter l'accès aux données concernées à une catégorie restreinte de personnes chargées d'accomplir certaines tâches pour le compte du CSIRT national</p>	<p>Paragraaf 2, tweede lid, bepaalt dat de leidende ambtenaren van het nationale CSIRT uitdrukkelijk de personen aanwijzen die gemachtigd zijn om bij de operatoren identificatie-, verkeers- of locatiegegevens op te vragen. Alleen de gemachtigde personen mogen deze gegevens ook verwerken. Doel van deze bepaling is ervoor te zorgen dat enkel een beperkte categorie van personen die bepaalde taken uitvoeren voor rekening van het nationale CSIRT, toegang krijgt tot de betrokken gegevens.</p>
Art. 35	Art. 35
<p>Cet article insère au sein du paragraphe 2 de l'article 65 de la loi NIS les termes « des données de communications électroniques » parmi les données pouvant être traitées par le CSIRT national, afin notamment de satisfaire au prescrit de l'article 23, §2, (b) du RGPD.]</p>	<p>Dit artikel voegt in paragraaf 2 van artikel 65 van de NIS-wet de woorden "elektronische communicatiegegevens" toe aan de gegevens die door het nationale CSIRT kunnen worden verwerkt, om met name te voldoen aan artikel 23, lid 2, (b), van de AVG.]</p>
CHAPITRE 10 - Entrée en vigueur	HOOFDSTUK 10 - Inwerkingtreding
Art. 36	Art. 36

[La loi prend effet rétroactivement afin de ne pas créer un vide juridique dans lequel des données importantes de communications électroniques qui pourraient être cruciales pour l'enquête ne soient plus conservées.]	[De wet treedt retroactief in werking, zodat er geen juridisch vacuüm ontstaat waardoor belangrijke elektronische communicatiegegevens die cruciaal zouden zijn voor het onderzoek, niet langer zouden bewaard worden.]
Par le Roi :	Van Koningswege :
Le premier,	De Eerste Minister,
Alexander DE CROO	
Le Vice-Premier Ministre et Ministre des Finances, chargé de la Coordination de la lutte contre la fraude,	De Vice-eersteminister en Minister van Financiën, belast met de Coördinatie van de fraudebestrijding,
Vincent VAN PETEGHEM	
Le Vice-Premier Ministre et Ministre des Affaires sociales et de la Santé publique,	De Vice-eersteminister en Minister van Sociale Zaken en Volksgezondheid,

Frank VANDENBROUCKE	
La Vice-Première Ministre et Ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,	De Vice-eersteminister en Minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,
Petra DE SUTTER	
Le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord,	De Vice-eersteminister en Minister van Justitie en Noordzee,
	
Vincent VAN QUICKENBORNE	
La Ministre de la Défense,	De Minister van Defensie,
Ludivine DEDONDER	

La Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique,	De Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing,
Annelies VERLINDEN	
Le secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée et de la Régie des bâtiments	De Staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy en met de Regie der gebouwen,
Mathieu MICHEL	