BELGISCH INSTITUUT VOOR POSTDIENSTEN EN TELECOMMUNICATIE

RAADPLEGING DOOR DE RAAD VAN HET BIPT VAN 31 JULI 2015 OP HET VERZOEK VAN DE VICE-EERSTEMINISTER EN DE MINISTER VAN DIGITALE AGENDA, TELECOMMUNICATIE EN POST BETREFFENDE HET VOORONTWERP VAN WET BETREFFENDE DE BEWARING VAN GEGEVENS IN DE ELEKTRONISCHE-COMMUNICATIESECTOR

WERKWIJZE OM REACTIES OP DIT DOCUMENT DOOR TE STUREN

Antwoordtermijn:	tot 31 augustus 2015
Wijze om te antwoorden:	Aan: consultation.sg@bipt.be Betreft: "Consult-2015-C7"

Aanspreekpunt: Pierre-Yves Dethy, juridisch adviseur (pierre-yves.dethy@ibpt.be)

Antwoorden dienen elektronisch te worden verzonden.

Er wordt gevraagd gebruik te maken van het "Formulier dat als voorpagina dient te worden gebruikt bij het antwoord op een door het BIPT georganiseerde openbare raadpleging" dat kan worden gevonden op het adres http://www.ibpt.be/nl/operatoren/telecom/markten/formulier-dat-als-voorpagina-dient-te-worden-gebruikt-bij-het-antwoord-op-een-door-het-bipt-georganiseerde-openbare-raadpleging

Het BIPT vraagt eveneens dat de opmerkingen verwijzen naar de paragrafen en/of delen waarop ze betrekking hebben.
Op het document moet duidelijk worden aangegeven wat vertrouwelijk is.

1. Context

Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken, en tot wijziging van Richtlijn 2002/58/EG, werd omgezet in Belgisch recht door de wet van 30 juli 2013 "houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering" (hierna de wet van 30 juli 2013) en door een koninklijk besluit[1].

Bij een arrest van 8 april 2014, heeft het Europese Hof van Justitie Richtlijn 2006/24/EG ongeldig verklaard[2]. Het Grondwettelijk Hof heeft, wat hem betreft, de wet van 30 juli 2013 volledig vernietigd met terugwerkende kracht bij een arrest van 11 juni 2005[3].

Naar aanleiding van deze nietigverklaring werd een voorontwerp van wet betreffende de bewaring van gegevens in de elektronische-communicatiesector voorbereid door de betrokken regeringsleden. Dat voorontwerp van wet werd bijgevoegd bij dit document.

Conform artikel 14.1 van de "Machtigingsrichtlijn"[4], moet een openbare raadpleging worden gehouden over het voorontwerp van wet. Deze wordt door het BIPT gehouden om het vereiste doelpubliek te bereiken (de elektronische-communicatiesector).

2. Doel van de raadpleging

De auteurs van het voorontwerp wensen de eventuele opmerkingen over de teksten in de bijlage te vergaren.

Op het verzoek van de auteurs van het voorontwerp van wet verzoekt het BIPT de bestemmelingen van de raadpleging eveneens om de volgende vragen te beantwoorden:

1) Ziet u andere elementen die het zouden mogelijk maken om rekening te houden met het arrest van 11 juni 2015 van het Grondwettelijk Hof?
2) Kan worden overwogen om een onderscheid te maken tussen de bewaringstermijnen voor gegevens in verband met de klassieke telefonie (nummer) en deze in verband met de datacommunicatie (bijvoorbeeld IP-adres)?
3) De overheden kunnen aan een operator vragen met welke mast(en) de telefoon van persoon X was verbonden tijdens een oproep of een sms op een gegeven ogenblik of wie allemaal was verbonden met een bepaalde mast op een gegeven moment in het kader van een oproep of een sms. Is het technisch mogelijk om deze gegevens op afzonderlijke wijze te bewaren?
4) Is het technisch mogelijk om een database bij te houden met de nummers die zijn verbonden met een Cell ID zelf, zonder een oproep of een sms? Zo ja, hoe lang zouden die gegevens kunnen worden bewaard?

[1] Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.
[2] C-293/12 en C-594/12.
[3] Gr. H., 11 juni 2015, nr. 84/2015.
[4] Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische-communicatienetwerken en -diensten ("Machtigingsrichtlijn").

5) Ziet u, in het kader van de technologische ontwikkelingen van uw netwerken, andere aandachtspunten die zouden moeten worden behandeld?

De raadpleging moet de betrokken regeringsleden in staat stellen om een besluit te nemen inzake de bewaringstermijnen: de termijnen die worden vermeld in de bijgevoegde documenten zijn in dit stadium indicatief.

3. Bijlagen

1) Memorie van toelichting bij het voorontwerp van wet betreffende de bewaring van gegevens in de elektronische-communicatiesector;
2) Dispositief van het voorontwerp van wet betreffende de bewaring van gegevens in de elektronische-communicatiesector.

Charles Cuvelliez
Raadslid

Axel Desmedt
Raadslid

Luc Vanfleteren
Raadslid

Jack Hamande
Voorzitter van de Raad

KONINKRIJK BELGIË

_____

Voorontwerp van wet betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie

SAMENVATTING

MEMORIE VAN TOELICHTING

Dames en heren,

ROYAUME DE BELGIQUE

_____

Avant-projet de loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques

RESUME

EXPOSE DES MOTIFS

Mesdames, Messieurs,

ALGEMEEN DEEL

1. **Inleiding**

Dit ontwerp van wet beoogt tegemoet te komen aan de vernietiging door het Grondwettelijk Hof van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna WEC), zoals gewijzigd bij de wet van 30 juli 2013. In het vernietigde artikel 126 WEC werd voorzien in de verplichting voor de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettelefoniediensten, internettoegangdiensten en internet-e-maildiensten om bepaalde gegevens te bewaren gedurende een termijn van twaalf maanden, opdat die gegevens beschikbaar zouden zijn voor bepaalde specifieke doeleinden en in het bijzonder voor de strafonderzoeken of onderzoeken met het oog op inlichtingen. De betrokken gegevens hebben geen betrekking op de inhoud van de communicaties.

Het arrest van het Grondwettelijk Hof ligt in het verlengde van de vernietiging door het Hof van Justitie van richtlijn 2006/24/EG, die in het vernietigde artikel 126 WEC ten uitvoer werd gelegd.

PARTIE GENERALE

1. **Introduction**

Le présent projet de loi vise à répondre à l'annulation par la Cour constitutionnelle de l'article 126 de la Loi du 13 juin 2005 relative aux communications électroniques (ci-après LCE), tel que modifié par la Loi du 30 juillet 2013. L'article 126 LCE annulé prévoyait l'obligation pour les fournisseurs au public de service de téléphonie fixe, mobile et par Internet, d'accès à Internet et courrier électronique par Internet de conserver certaines données pendant une durée de 12 mois afin que ces données soient disponibles pour certaines finalités précises et en particulier pour les enquêtes pénales ou de renseignement. Les données en question ne concernent pas le contenu des communications.

L'arrêt de la Cour constitutionnelle se situe dans le prolongement de l'annulation par la Cour de justice de la directive 2006/24/CE que l'article 126 LCE annulé mettait en œuvre.

2. **Huidige situatie**

Het vernietigde artikel 126 komt voort uit de wet van 30 juli 2013. Wegens de vernietiging ervan wordt het geacht nooit te hebben bestaan en is het vroegere artikel 126, dat werd ingevoegd door de eerste versie van de WEC, van toepassing. In dat oorspronkelijke artikel 126 WEC werd reeds voorzien in het algemene beginsel van de verplichting tot het bewaren van bepaalde elektronische gegevens. Het was echter minder duidelijk dan het vernietigde artikel 126. Die situatie schenkt geen voldoening.

Bovendien moet eraan worden herinnerd dat een groot deel van de gegevens bedoeld in artikel 126 WEC (ongeacht de versie ervan) ook wordt bedoeld in artikel 122 WEC: het Belgisch recht biedt (net als het Europees recht) de operatoren immers de mogelijkheid om die gegevens, met inachtneming van een reeks voorwaarden, te bewaren voor commerciële doeleinden (inzonderheid marketing of facturering).

3. Belang van de communicatiegegevens voor de strafonderzoeken en de onderzoeken met het oog op inlichtingen

De gegevens met betrekking tot de communicaties spelen een steeds grotere rol in de strafonderzoeken en de onderzoeken met het oog op inlichtingen. Dat heeft uiteraard te maken met het gegeven dat de nieuwe communicatietechnologieën een steeds grotere plaats innemen in het leven van de burgers.

Die nieuwe technologieën reiken niet alleen de onderzoekers nieuwe instrumenten aan, maar ook de criminelen, die rechtstreeks via die nieuwe technologieën misdrijven kunnen plegen of misdrijven grotendeels kunnen voorbereiden via die communicaties.

Vóór de opkomst van de mobiele telefonie en het internet waren de identificatie van een abonnee van een vaste telefoonlijn en de toegang tot het overzicht van de telefoongesprekken reeds een vrij gebruikelijke maatregel in het kader van de onderzoeken. Door de toenmalige situatie in de

2. **La situation actuelle**

L'article 126 annulé provient de la loi du 30 juillet 2013. En raison de son annulation, il est censé n'avoir jamais existé et l'ancien article 126, inséré par la première version de la LCE est d'application. Cet article 126 LCE initial prévoyait déjà le principe général de l'obligation de conservation de certaines données électroniques. Il était toutefois moins précis que l'article 126 annulé. Cette situation n'est pas satisfaisante.

Il faut par ailleurs rappeler qu'une partie importante des données visées par l'article 126 LCE (quelle que soit sa version) est aussi visée par l'article 122 LCE : le droit belge (comme le droit européen), permet en effet aux opérateurs de conserver ces données, en respectant une série de conditions, à des fins commerciales (notamment le marketing ou la facturation).

3. L'importance des données de communication pour les enquêtes pénales et de renseignement

Les données relatives aux communications jouent un rôle croissant dans les enquêtes pénales et de renseignement. C'est bien sûr lié à la place croissante des nouvelles technologies de communication dans la vie des citoyens.

Ces nouvelles technologies offrent certes des outils nouveaux pour les enquêteurs mais aussi aux criminels qui soit peuvent commettre des infractions directement via ces nouvelles technologies soit peuvent préparer des infractions en grande partie via ces communications.

Avant l'émergence de la téléphonie mobile et d'Internet, l'identification d'un abonné d'une ligne de téléphonie fixe et l'accès à l'historique des appels téléphoniques étaient déjà une mesure assez routinière dans les enquêtes. La situation du secteur des télécommunications à l'époque et les

sector van de telecommunicatie en de behoeften inzake facturering werden de gegevens gedurende een vrij lange periode bewaard, zodat het nooit nodig is geweest om in wetgeving te voorzien. De gevoeligheid was niet dezelfde (de overgrote meerderheid van de abonnees was zelfs vermeld in de telefoongids). De toegang tot dat type gegevens is dus niet nieuw en het belang ervan in het kader van de onderzoeken al evenmin. Dat belang is daarentegen nog groter geworden door de explosie van het aantal communicaties, zulks ondanks de eveneens groeiende bekommernis inzake de persoonlijke levenssfeer.

besoins en facturation faisaient que les données étaient conservées durant une période assez longue de sorte qu'il n'a jamais été nécessaire de légiférer. La sensibilité n'était pas la même (au point que la très grande majorité des abonnés était reprise dans l'annuaire téléphonique). L'accès à ce type de données n'est donc pas nouveau, pas plus que leur importance dans les enquêtes. Celle-ci s'est au contraire renforcée avec l'explosion de la masse des communications même si la préoccupation en matière de vie privée va également croissant.

De behoefte om de houder van een gsm-nummer of van een IP-adres te identificeren, is een gebruikelijk aspect van de onderzoeken en een absoluut noodzakelijk onderdeel ervan geworden. De toegang tot het overzicht van de communicaties of de lokalisatie a posteriori van de verdachte of van het slachtoffer zijn maatregelen die de persoonlijke levenssfeer meer aantasten en die minder worden gebruikt dan de identificatie, maar zij zijn niettemin zeer vaak absoluut noodzakelijk in bepaalde soorten zaken.

Le besoin d'identifier le titulaire d'un numéro de gsm ou d'une adresse IP est devenu un aspect routinier des enquêtes et une étape indispensable de celles-ci. L'accès à l'historique des communications ou la localisation a posteriori du suspect ou de la victime sont des mesures plus attentatoires à la vie privée et moins utilisées que l'identification mais sont néanmoins très souvent indispensables dans certains types d'affaires.

Het ontwerp van wet heeft geen betrekking op de inhoud van de communicaties.

Le contenu des communications n'est pas visé par le projet de loi.

De sector van het terrorisme is uiteraard bijzonder actueel. De toegang tot de communicatiegegevens is een noodzakelijke stap voor het identificeren van de personen en de banden die zij onderling hebben. Wanneer bij een huiszoeking een hele zak simkaarten wordt ontdekt of een draagbare computer in beslag wordt genomen, wordt vervolgens een groot aantal onderzoekshandelingen verricht om de communicaties na te trekken die met die elementen zijn verricht en daarna met andere aldus geïdentificeerde elementen, enz. Dergelijke maatregelen zijn ook onontbeerlijk wanneer een persoon die nog niet bekend was bij de politie- of inlichtingendiensten zich blijkt te hebben aangesloten bij een terroristische organisatie in Syrië bijvoorbeeld. Tot slot is het bij het onderzoek na een aanslag uiteraard noodzakelijk om terug te gaan in de communicaties van de verdachte, inzonderheid om na te gaan of hij alleen heeft gehandeld of om medeplichtigen te identificeren.

Le secteur du terrorisme est évidemment particulièrement d'actualité. L'accès aux données de communication est une étape incontournable pour identifier les personnes et les liens entre celles-ci. Lorsqu'une perquisition mène à la découverte d'un sac entier de cartes SIM ou la saisie d'un ordinateur portable, il s'ensuite un grand nombre d'actes d'enquêtes pour retracer les communications passées à partir de ces éléments puis à partir d'autres éléments ainsi identifiés, etc. Ce type de mesures sera aussi indispensable lorsqu'une personne qui n'était pas encore connue des services de police ou de renseignement s'avère avoir rejoint les rangs d'une organisation terroriste en Syrie par exemple. Enfin, l'enquête après un attentat impose évidemment de revenir en arrière dans les communications du suspect pour notamment vérifier s'il a agi seul ou identifier des complices.

De andere sector die zeer vaak wordt vermeld om het belang van die gegevens te illustreren is die van de kinderpornografie. Ook hier moet kunnen worden teruggegaan in de tijd om op basis van de detectie van een element op het internet het volledige netwerk te kunnen blootleggen.

Maar uit die bijzonder sprekende voorbeelden mag niet worden afgeleid dat de gegevens enkel noodzakelijk zijn voor het bestrijden van weliswaar choquerende maar in aantal relatief beperkte fenomenen van criminaliteit. De realiteit is dat de communicatiegegevens nodig zijn in zeer veel verschillende situaties waarin men zich evenwel gemakkelijk kan inbeelden dat die gegevens vaak zowel het vertrekpunt als een fase van het onderzoek zijn, bijvoorbeeld:

- de reactie op een onrustwekkende verdwijning;
- de illegale handel in verdovende middelen;
- de verkoop van namaakgeneesmiddelen op het internet;
- het aanzetten tot haat of geweld;
- belaging, ook bij jongeren;
- spionage, die, net als rekrutering, over verschillende jaren kan zijn gespreid, en hacking voor spionagedoeleinden, kan pas verschillende maanden na de feiten aan het licht komen;
- hacking van bankrekeningen;
- identiteitsdiefstal;
- hacking waarbij bijvoorbeeld wordt gechanteerd met de bekendmaking van de verzamelde persoonsgegevens of commerciële gegevens;
- enz.

Daaraan moet een belangrijke factor worden toegevoegd die het tijdselement en de behoefte om terug te gaan in de tijd beïnvloedt. Die factor is de lokalisatie van de aanbieders van diensten via het internet en het gegeven dat sommige van die diensten die in het buitenland gebaseerd zijn, eisen dat een beroep wordt gedaan op de formele justitiële samenwerking met het oog op de overzending van gegevens. De justitiële samenwerking, inzonderheid met de Verenigde Staten, is echter een zeer zwaar en zeer traag proces. België probeert de situatie te verbeteren maar heeft uiteraard niet alle kaarten in handen. Met dat gegeven moet dan ook rekening worden gehouden.

L'autre secteur très souvent mentionné pour illustrer l'importance de ces données est celui de la pédopornographie. Ici aussi, il faut pouvoir remonter dans le temps à partir de la détection d'un élément sur Internet pour pouvoir mettre à jour l'ensemble du réseau.

Mais ces exemples particulièrement parlants ne doivent pas laisser penser que les données sont nécessaires uniquement pour lutter contre des phénomènes de criminalité certes choquants mais relativement limités en nombre. La réalité est que les données de communications sont nécessaires dans une grande variété de situations mais où on imagine aisément que ces données sont souvent à la fois le point de départ et une étape de l'enquête, par exemple :

- La réaction à une disparition inquiétante ;
- Le trafic de stupéfiants ;
- La vente par Internet de médicaments contrefaits ;
- Les incitations à la haine ou à la violence ;
- Le harcèlement, y compris chez les jeunes ;
- L'espionnage qui peut s'étaler sur plusieurs années de même que le recrutement et où le hacking à des fins d'espionnage peut être découvert plusieurs mois après qu'il ait eu lieu ;
- Le piratage de comptes bancaires ;
- Le vol d'identité ;
- Le hacking associé par exemple au chantage de la divulgation des données personnelles ou commerciales collectées ;
- Etc.

Il faut ajouter à cela un facteur majeur qui influence l'élément temporel et le besoin de revenir dans le passé. Ce facteur est celui de la localisation des fournisseurs de service par Internet et le fait que certains de ces services basés à l'étranger exigent le passage par la coopération judiciaire formelle pour transmettre des données. Or le passage par la coopération judiciaire, notamment avec les Etats-Unis est un processus très lourd et très lent. La Belgique tente d'améliorer la situation mais n'a évidemment pas toutes les cartes en main. Cet élément doit donc être pris en compte.

Door die situatie duurt het vaak verschillende maanden om van een aanbieder van diensten via het internet het IP-adres te krijgen vanwaar een bericht bijvoorbeeld werd verstuurd. Pas vanaf dat moment kunnen de Belgische onderzoekers toegang vragen tot de identificatiegegevens op basis van het betrokken IP-adres.

De toegang tot de communicatiegegevens is dus onontbeerlijk, net als de mogelijkheid om voor een bepaalde periode te kunnen teruggaan in de tijd. Dat hangt uiteraard af van de bewaartermijn van de gegevens.

Cette situation fait qu'il faudra souvent plusieurs mois pour obtenir d'un fournisseur de services par Internet l'adresse IP à partir de laquelle un message par exemple a été posté. Ce n'est qu'à partir de ce moment que les enquêteurs belges peuvent demander l'accès aux données d'identification sur base de l'adresse IP en question.

L'accès aux données de communication est donc indispensable tout comme la possibilité de pouvoir remonter dans le passé pour une certaine période. Cela dépend forcément de la durée de conservation des données.

4. Het bewaren van de gegevens is geen grootschalig toezicht

Het lijdt geen twijfel dat de verplichting om de communicatiegegevens te bewaren een aanzienlijke beperking vormt van de persoonlijke levenssfeer van de individuen en in dat opzicht belangrijke garanties en beperkingen vereist.

Het is echter van essentieel belang dat die bewaarplicht niet wordt verward met het grootschalige toezicht dat bepaalde landen bewerkstelligen en waarover de pers regelmatig nieuwe onthullingen doet. Dat toezicht wordt gekenmerkt door het gegeven dat buitenlandse diensten een gigantisch aantal gegevens daadwerkelijk filteren en verwerken.

De in dit ontwerp van wet beoogde maatregel heeft niets te maken met dat soort aanpak. Hoewel de bewaring effectief alle burgers treft voor zover zij gebruik maken van een telefoon of van het internet, zullen de toegang en het gebruik van hun gegevens steeds gericht zijn en beperkt zijn tot een concreet geval, voor het verwezenlijken van een van de doeleinden waarin is voorzien, in het bijzonder in het kader van een strafonderzoek of een onderzoek met het oog op inlichtingen. Die toegang wordt verleend onder gerechtelijk toezicht wat het strafonderzoek betreft of onder toezicht van een onafhankelijke commissie (BIM-commissie) wat het onderzoek met het oog op inlichtingen betreft. Misbruiken zijn strafbaar. De

4. La conservation des données n'est pas de la surveillance de masse

Il ne fait pas de doute que l'obligation de conserver les données de communication constitue une limitation majeure de la vie privée des individus et nécessite à cet égard des limitations et des garanties importantes.

Il est toutefois essentiel de ne pas confondre cette obligation de conservation avec la surveillance de masse réalisée par certains pays et pour laquelle la presse apporte régulièrement de nouvelles révélations. Cette surveillance est caractérisée par le fait que des services étrangers filtrent et traitent effectivement un nombre gigantesque de données.

La mesure visée par le présent projet de loi ne relève pas du tout de ce type d'approche. Si la conservation touche effectivement tous les citoyens pour autant qu'ils utilisent un téléphone ou Internet, l'accès à et l'utilisation de leurs données seront toujours ciblé et limité à un cas concret pour l'exercice d'une des finalités prévues, en particulier dans le cadre d'une enquête pénale ou de renseignement. Cet accès se fait sous contrôle judiciaire pour l'enquête pénale ou sous contrôle d'une commission indépendante (Commission BIM) pour le renseignement. Les abus sont punissables. Il sera en outre toujours limité dans le temps avec un maximum de 12 mois pour les données d'identification et des délais plus

toegang zal bovendien steeds beperkt zijn in de tijd, met een maximum van 12 maanden voor de identificatiegegevens en kortere termijnen voor de andere gegevens.

courts pour les autres données.

5. Bewaren en verwerken van gegevens voor commerciële doeleinden

Het belang van de verplichting tot het bewaren van de gegevens en van de impact ervan op de persoonlijke levenssfeer mag in geen geval worden geminimaliseerd. Dit ontwerp van wet stoelt volledig op het besef dat het om een gevoelige maatregel gaat en dat de nodige garanties moeten worden geboden.

5. La conservation et le traitement de données à des fins commerciales

Il ne saurait être question de minimaliser l'importance de l'obligation de conservation des données et son impact sur la vie privée. Le présent projet de loi est tout entier fondé sur la conscience de la sensibilité de la mesure et la nécessité d'apporter les garde-fous nécessaires.

Er moet evenwel erop worden gewezen dat de burgers bij het nemen van een abonnement voor telefonie of internettoegang ermee instemmen dat de operator de communicatiegegevens die nodig zijn zowel voor de facturering als voor marketingdoeleinden bewaart zolang het nodig is voor die doeleinden. Dat is legitiem, uitdrukkelijk toegestaan en geregeld in artikel 122 WEC op grond waarvan artikel 6 van richtlijn 2002/58/EG wordt omgezet (richtlijn "privacy en elektronische communicatie"). Het lijdt echter geen twijfel dat de gegevens die de operatoren bewaren op grond van artikel 122 WEC kunnen worden gebruikt met het oog op het strafonderzoek of met het oog op inlichtingen, onder de voorwaarden waarin is voorzien in die wettelijke kaders.

Il faut néanmoins rappeler que les citoyens, en souscrivant les abonnements de téléphonie ou d'accès à Internet, consentent à ce que les données de communication nécessaires non seulement à la facturation mais aussi au marketing soient conservées par l'opérateur aussi longtemps que cela est nécessaire pour ces finalités. Cela est légitime et explicitement autorisé et réglé par l'article 122 LCE qui transpose l'article 6 de la directive 2002/58/CE (directive « vie privée et communications électroniques »). Or il ne fait pas de doute que les données conservées par les opérateurs sur base de l'article 122 LCE peuvent être utilisées pour les finalités de l'enquête pénale ou du renseignement, dans les conditions prévues par ces cadres légaux.

Het bewaren van de gegevens door de operator op die basis is meestal het resultaat van een berekening van de kosten en de baten. De Europese werkzaamheden inzake het bewaren van de gegevens zijn in grote mate het gevolg van de bewustwording van de politiële en gerechtelijke overheden van het gegeven dat die situatie hen volledig afhankelijk maakte van de commerciële strategieën van de operatoren. Die strategieën evolueren evenwel. Zo waren bij het verschijnen van de 'flat rate'-abonnementen bepaalde gegevens die tot dan toe werden bewaard door de operatoren met het oog op facturering (en die dus toegankelijk waren in het gerechtelijke kader of in het kader van inlichtingen) niet langer nodig voor die facturering, terwijl zij belangrijk blijven voor de onderzoeken.

La conservation des données sur cette base par l'opérateur est le plus souvent le résultat d'un calcul coût / bénéfice. Les travaux européens sur la conservation des données ont en grande partie été provoqués par la prise de conscience des autorités policières et judiciaires du fait que cette situation les rendait entièrement dépendantes des stratégies commerciales des opérateurs. Or ces stratégies évoluent. Ainsi, avec l'apparition des abonnements « flat rate », certaines données jusqu'alors conservées par les opérateurs aux fins de facturation (et donc accessibles dans le cadre judiciaire ou de renseignement) n'étaient plus nécessaires pour cette finalité de facturation alors qu'elles restent importantes pour les enquêtes.

De burgers vertrouwen overigens steeds meer elektronische gegevens, die soms uiterst gevoelig zijn, toe aan private actoren (Facebook bijvoorbeeld, maar ook de berichten- of opslagsystemen in de 'cloud'). Die private actoren krijgen van hun gebruikers de toestemming voor de onafgebroken verwerking van steeds grotere hoeveelheden persoonsgegevens waarmee men heel veel over de persoon te weten kan komen bij het combineren ervan.

Les citoyens confient par ailleurs de plus en plus de données électroniques parfois extrêmement sensibles à des acteurs privés (Facebook par exemple mais aussi les systèmes de messagerie ou de stockage dans le « cloud Ces acteurs privés reçoivent de leurs utilisateurs l'autorisation de traiter de manière continue des données personnelles de plus en plus massives et dont la combinaison permet de savoir énormément de choses sur la personne.

Dat moet uiteraard niet leiden tot meer bevoegdheden voor de gerechtelijke overheden of de inlichtingendiensten. De burger moet bewust worden gemaakt van het beheer van zijn persoonsgegevens op het internet en er mag niet worden geconcludeerd dat het prijsgeven van de persoonlijke levenssfeer het versterkt toezicht door de diensten van de staat zou verantwoorden. Toch is het nuttig om een gezonde waakzaamheid aan de dag te leggen ten aanzien van de verplichting tot het bewaren van de gegevens voor hoofdzakelijk gerechtelijke doeleinden of met het oog op inlichtingen, in het licht van die tolerantie van een meerderheid van de burgers ten aanzien van de stelselmatige verwerking van hun gegevens door private actoren voor commerciële doeleinden.

Ceci ne doit évidemment pas amener à démultiplier les pouvoirs des autorités judiciaires ou des services de renseignement. Il faut sensibiliser le citoyen à la gestion de ses données personnelles sur Internet et on ne saurait conclure à un renoncement à la vie privée qui justifierait la surveillance accrue par les services de l'Etat. Néanmoins, il est utile de mettre en perspective la saine vigilance face à l'obligation de conservation des données pour des finalités principalement judiciaires ou de renseignement en la confrontant à cette tolérance d'une majorité des citoyens face au traitement systématique de leurs données par des acteurs privés pour des motifs commerciaux.

6. Kritieken van het Grondwettelijk Hof

De argumentatie van het Grondwettelijk Hof is zeer kort en verwijst vooral naar de beslissing van het Hof van Justitie van de EU betreffende de richtlijn 2006/24/EG.

Het Hof besluit dat het bestreden artikel 126 WEC, net als de richtlijn, een onevenredige beperking van het recht op de eerbiediging van de persoonlijke levenssfeer inhoudt. Die schending van het evenredigheidsbeginsel vloeit voort uit de combinatie van vier elementen:

- het gegeven dat de bewaring van de gegevens voor alle personen geldt;
- het gebrek aan differentiatie op grond van de categorieën van bewaarde gegevens en het nut ervan;
- het gebrek aan of de ontoereikendheid van

6. Les critiques adressées par la Cour constitutionnelle

L'argumentaire de la Cour constitutionnelle est très bref et renvoie surtout à la décision de la Cour de justice UE concernant la directive 2006/24/CE.

La Cour conclut que l'article 126 LCE attaqué, comme la directive, constitue une limitation disproportionnée du droit au respect de la vie privée. Cette violation du principe de proportionnalité découle de la combinaison de quatre éléments :

- Le fait que la conservation des données concerne toutes les personnes ;
- L'absence de différenciation en fonction des catégories de données conservées et leur utilité ;
- L'absence ou l'insuffisance de règles quant à

regels inzake de toegang van de overheden tot de betrokken gegevens;

- en tot slot, hoewel dit element enkel wordt aangehaald door het Hof van Justitie en niet door het Grondwettelijk Hof, het gebrek aan of het tekortschieten van de regels inzake de beveiliging van de gegevens bij de aanbieders of de operatoren.

Die elementen en de antwoorden die het ontwerp van wet daarop biedt, worden hierna overlopen.

7. Onderscheid op grond van de personen, periodes en geografische zones

Het eerste van de drie elementen waarvan de combinatie het evenredigheidsbeginsel schendt, betreft het beginsel zelf van de verplichting tot het bewaren van de gegevens. Het gaat erom dat de gegevens van alle personen op ongedifferentieerde wijze worden bewaard. Na grondige analyse blijkt dat dat een a priori differentiatie van dit element niet mogelijk is.

a) Alle personen, ook al zijn zij nog niet betrokken bij een onderzoek

De bewaring van de gegevens beperken tot de gegevens betreffende personen ten aanzien van wie reeds een strafonderzoek of een onderzoek met het oog op inlichtingen loopt, heeft geen zin want die mogelijkheid bestaat overigens reeds. De gerechtelijke overheden en de inlichtingendiensten kunnen het 'doen opsporen' van de communicaties reeds opleggen in het kader van een specifiek onderzoek en dus de operatoren en aanbieders van toegang verplichten tot het bewaren van de gegevens voor de toekomst, zodra de persoon of een communicatiedienst is geïdentificeerd in een strafonderzoek. Het doel van artikel 126 WEC bestaat erin zich ervan te vergewissen dat een bepaald aantal gegevens ook voor een beperkte periode van het verleden beschikbaar zijn. Artikel 126 heeft dus enkel zin indien het betrekking heeft op de personen ten aanzien van wie nog niet noodzakelijkerwijs een strafonderzoek of een onderzoek met het oog op inlichtingen loopt.

Die dimensie is absoluut noodzakelijk, zoals de in punt 2 vermelde voorbeelden aantonen.

l'accès des autorités aux données concernées ;

- Et enfin, bien que cet élément soit soulevé seulement par la Cour de justice et pas par la Cour constitutionnelle, l'absence ou la faiblesse des règles sur la sécurisation des données chez les fournisseurs ou les opérateurs.

Ces éléments, et les réponses que le projet de loi y apporte, sont passés en revue ci-dessous.

7. La distinction en fonction des personnes, périodes temporelles et zones géographiques

Le premier des trois éléments dont la combinaison viole le principe de proportionnalité concerne le principe même de l'obligation de conservation des données. C'est le fait de conserver les données de toutes les personnes de manière indifférenciée. Après analyse approfondie, il ressort qu'il n'est pas possible d'opérer une différenciation a priori de cet élément.

a) Toutes les personnes même si elles ne sont pas encore impliquées dans une enquête

Limiter la conservation des données à celles concernant des personnes qui font déjà l'objet d'une enquête pénale ou de renseignement n'a pas de sens car cette possibilité existe déjà par ailleurs. Les autorités judiciaires comme les services de renseignement peuvent déjà imposer le « repérage » des communications dans le cadre d'une enquête précise et donc obliger les opérateurs et fournisseurs d'accès à conserver les données pour le futur une fois qu'on a identifié la personne ou un service de communication dans une enquête pénale. L'objectif de l'article 126 LCE est de s'assurer qu'un certain nombre de données existeront aussi pour une période limitée du passé. L'article 126 n'a donc de sens que s'il porte sur les personnes qui ne font pas encore nécessairement l'objet d'une enquête pénale ou de renseignement.

Cette dimension est indispensable comme le montrent les exemples repris au point 2.

Er moet trouwens erop worden gewezen dat de maatregel zowel in het voordeel kan zijn van het slachtoffer, voor zijn eigen gegevens (in zaken met betrekking tot belaging bijvoorbeeld 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 decharge kan meespelen.

Il faut par ailleurs rappeler que la mesure peut tout aussi bien bénéficier à la victime pour ses propres données (dans des affaires de harcèlement par exemple, il s'agira de retourner dans le passé des données de la victime pour identifier l'origine d'un appel, un email ou un sms) que l'accusé (les données de localisation peuvent montrer que l'accusé n'était pas sur le lieu de l'infraction au moment où elle a été commise). Il peut aussi s'agir d'identifier des témoins ce qui peut jouer à charge comme à décharge.

b) Geen differentiatie op grond van de periode, de geografische zone of een kring van personen

Het Grondwettelijk Hof, dat verwijst naar het arrest van het Hof van Justitie, wijst erop dat het bestreden artikel 126 "de bewaring van de desbetreffende gegevens [evenmin beperkt] tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een door de wet beoogde inbreuk, of die zouden kunnen helpen, door het bewaren van de gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken".

Dit deel van het arrest van het Hof van Justitie leidde tot nogal wat vragen over de draagwijdte ervan. De werkgroep die dit ontwerp van wet heeft voorbereid, heeft zich eveneens vragen gesteld over de mogelijkheid de impact van artikel 126 te beperken door te werken aan de door het Hof van Justitie aangehaalde criteria, te weten "een bepaalde periode", "een bepaalde geografische zone" of nog "een kring van personen".

Het besluit is dat dit deel van het arrest van het Hof van Justitie moet worden gelezen als een verklaring voor de gevoeligheid van het beginsel van veralgemeende bewaring van de gegevens. Het is evenwel niet mogelijk een oplossing eraan te ontlenen om een differentiatie toe te passen.

De verwijzing naar de "periode" zou bijvoorbeeld een specifieke en tijdelijke situatie van bedreiging van de openbare orde of veiligheid kunnen beogen. Enerzijds is dit type criterium evenwel niet coherent met een groot aantal situaties en types van criminaliteit waarvoor de bewaring van de gegevens doorslaggevend blijkt te zijn

b) Pas de différenciation en fonction de la période temporelle, la zone géographique ou un cercle de personnes

La Cour constitutionnelle, renvoyant à l'arrêt de la Cour de justice, note que l'article 126 attaqué « ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d'être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions ».

Cette partie de l'arrêt de la Cour de justice a suscité beaucoup d'interrogations quant à sa portée. Le groupe de travail qui a préparé le présent projet de loi s'est lui aussi interrogé sur la possibilité de limiter l'impact de l'article 126 en travaillant sur les critères soulevés par la Cour de justice, c'est-à-dire une « période temporelle », « une zone géographique déterminée » ou encore « un cercle de personnes ».

La conclusion est que cette partie de l'arrêt de la Cour de justice doit être lue comme une explication de la sensibilité du principe de conservation généralisée des données. Mais il n'est pas possible d'y puiser une solution pour appliquer une différenciation.

La référence à la « période temporelle » pourrait par exemple viser une situation spécifique et temporaire de menace pour l'ordre ou la sécurité publique. Mais, d'une part, ce type de critère n'est pas cohérent avec un grand nombre de situations et de types de criminalité pour lesquels la conservation des données s'avère décisive (par

(bijvoorbeeld inzake kinderpornografie) en anderzijds zou dit type criterium, daar waar het van toepassing zou kunnen zijn, geen rekening houden met het gegeven dat er niet noodzakelijkerwijs kan worden vooruitgelopen op de betrokken situatie (bijvoorbeeld in geval van een terroristische dreiging die wordt geconcretiseerd door een aanslag).

exemple en matière de pédopornographie) et, d'autre part, là où il pourrait trouver à s'appliquer, ce type de critère négligerait le fait que la situation en question ne peut pas forcément être anticipée (par exemple en cas de menace terroriste matérialisée par un attentat).

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.

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.

c) Geen uitsluiting van bepaalde beroepen

Het Grondwettelijk Hof wijst, nog steeds met betrekking tot dat gebrek aan differentiatie tussen de personen van wie de gegevens worden bewaard, ten slotte erop dat "de wet, zonder enige uitzondering, ook van toepassing [is] op personen van wie de communicaties onder het beroepsgeheim vallen".

c) Pas d'exclusion de certaines professions

La Cour constitutionnelle note enfin, toujours concernant cette absence de différenciation entre les personnes dont les données sont conservées, que « la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel ».

Ook hier rees de vraag naar de mogelijkheid te voorzien in een differentiatie om gevolg te geven aan dit deel van het arrest. Het zou erom gaan a priori bepaalde personen op grond van hun beroep niet in aanmerking te nemen voor de bewaring van de gegevens.

Ici aussi, on s'est interrogé sur la possibilité de créer une différentiation pour faire suite à cette partie de l'arrêt. Il s'agirait d'exclure a priori certaines personnes, en fonction de leur profession, de la conservation des données.

Die differentiatie is niet mogelijk. Hoewel het klopt dat bepaalde beroepen worden beschermd inzake het verzamelen van bewijzen of inlichtingen, is die bescherming nooit absoluut. Langs de andere kant moet hier nog worden opgemerkt dat de bewaring van de gegevens niet mag worden gezien als een maatregel die strekt tot een toegang a posteriori tot de gegevens, noodzakelijkerwijs "tegen" de persoon. Het betrokken gegeven kan worden gebruikt om die persoon vrij te pleiten of nog nuttig zijn wanneer de betrokken persoon het slachtoffer is van een misdrijf. Er moet opnieuw worden opgemerkt dat de bewaring van de gegevens geen betrekking heeft op de inhoud van de communicaties.

Cette différentiation n'est pas possible. D'une part, s'il est vrai que certaines professions sont protégées en matière de collecte de la preuve ou de renseignement, cette protection n'est jamais absolue. D'autre part, il faut ici encore noter que la conservation des données ne peut pas être vue comme une mesure visant un accès a posteriori aux données nécessairement « contre » la personne. La donnée en question peut servir à disculper celle-ci ou encore être utile lorsque la personne en question est victime d'une infraction. Rappelons à nouveau que la conservation des données ne concerne pas le contenu des communications.

Verder in de tekst zal evenwel blijken dat de

On verra toutefois plus loin que la protection de

bescherming van bepaalde beroepen wordt versterkt in dit ontwerp van wet maar op het niveau van de regelgeving inzake de toegang tot de bewaarde gegevens.

certaines professions est bien renforcée dans le présent projet de loi mais au niveau de la réglementation de l'accès aux données conservées.

Er kan worden geconcludeerd dat het niet mogelijk is artikel 126 WEC nader toe te passen op grond van het door het Grondwettelijk Hof en het Hof van Justitie aangehaalde eerste element (geen differentiatie op grond van de personen). Alle Europese landen waarmee contact werd opgenomen, zijn tot dezelfde conclusie gekomen.

On peut conclure qu'il n'est pas possible de modaliser l'article 126 LCE sur base du premier élément (l'absence de différentiation en fonction des personnes) repris par la Cour constitutionnelle et la Cour de justice. Tous les pays européens contactés sont arrivés à la même conclusion.

Noch in het arrest van het Grondwettelijk Hof, noch in dat van het Hof van Justitie van de EU wordt evenwel geconcludeerd dat slechts één van de vier elementen volstaat om een schending van het evenredigheidsbeginsel in te houden. Indien dit het geval zou zijn en aangezien het gebrek aan differentiatie tussen de personen het essentiële element vormt van de vernietigde Europese en nationale wetgeving, kan worden gedacht dat het Hof van Justitie en het Grondwettelijk Hof enkel dit aspect zouden hebben onderzocht en tot een schending van het recht op eerbiediging van de persoonlijke levenssfeer zouden hebben besloten zonder de andere elementen te onderzoeken.

Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice UE ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.

De verschillende elementen aangehaald door het Hof van Justitie van de EU en het Grondwettelijk Hof moeten dan ook worden gecombineerd. Aangezien het beginsel van de veralgemeende bewaring (met andere woorden zonder differentiatie tussen de personen) van de communicatiegegevens op zich een zeer belangrijke beperking van het recht op eerbiediging van de persoonlijke levenssfeer vormt, moet dit element worden "gecompenseerd" door een striktere regeling inzake de andere aspecten.

Il faut donc combiner les différents éléments soulevés par la Cour de justice UE et la Cour constitutionnelle. Puisque le principe de la conservation généralisée (c'est-à-dire sans différenciation entre les personnes) des données de communication constitue en soi une limitation très importante du droit au respect de la vie privée, il faut « compenser » cet élément par un régime plus strict sur les autres aspects.

8. Differentiatie op grond van de categorieën van gegevens

Het Grondwettelijk Hof wijst erop dat "[w]at [...] de bewaarperiode van de gegevens betreft, [...] de wet geen enkel onderscheid [maakt] tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen". Alle

8. La différenciation en fonction des catégories de données

La Cour constitutionnelle note que « […] en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées ». Toutes les données

gegevens waarvoor de bewaarplicht geldt, worden immers bewaard voor een unieke duur van 12 maanden in de vernietigde wet.

faisant l'objet de l'obligation de conservation sont en effet conservées pour une durée unique de 12 mois dans la loi annulée.

Dit ontwerp van wet vult deze leemte aan en voert een onderscheid in op grond van vier categorieën van gegevens.

Le présent projet de loi comble cette lacune et introduit une distinction sur base de 4 catégories de données.

De eerste categorie betreft de identificatiegegevens (wie is houder van een bepaald gsm-nummer, wat is het gsm-nummer van een bepaalde persoon, wie zit er achter een bepaald IP-adres, enz.). Die gegevens, die het meest worden gevraagd en de persoonlijke levenssfeer op matige wijze aantasten, in vergelijking met inzonderheid de derde en vierde categorie, moeten maximaal 12 maanden worden bewaard.

La première catégorie concerne les données d'identification (qui est titulaire de tel numéro de gsm, quel est le numéro de gsm de telle personne, qui se trouve derrière telle adresse IP, …). Ces données, qui sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux troisième et quatrième catégories, devront être conservées pour une durée maximale de 12 mois.

De tweede categorie betreft de gegevens met betrekking tot de communicatiediensten (bijvoorbeeld de verbruikte volumes). Aangezien die gegevens minder nuttig zijn dan de andere categorieën is het normaal dat een beperktere bewaring wordt opgelegd. Zij moeten maximaal 2 maanden worden bewaard.

La deuxième catégorie concerne les données relatives aux services de communication (par exemple les volumes consommés). Ces données étant d'une utilité moindre que les autres catégories, il est normal d'imposer une conservation plus limitée. Elles devront être conservées pendant 2 mois maximum.

De derde categorie en de vierde categorie zijn onderling afhankelijk en worden samen behandeld.

La troisième catégorie et la quatrième catégories sont interdépendantes et sont traitées ensemble.

De derde categorie betreft de verbindings- en lokalisatiegegevens (wat is inzonderheid de plaats en de duur van een communicatie).

La troisième catégorie concerne les données de connexion et localisation (quel est notamment le lieu et la durée d'une communication).

De vierde categorie betreft de persoonlijke communicatiegegevens (wie heeft gebeld of gecorrespondeerd met wie).

La quatrième catégorie concerne les données personnelles de communications (qui a appelé ou correspondu avec qui).

De derde en vierde categorie tasten de persoonlijke levenssfeer meer aan dan de andere twee categorieën. De toegangen tot die gegevens zijn minder talrijk dan die tot de identificatiegegevens maar blijven frequent. Die gegevens moeten [9/12] maanden worden bewaard.

Les troisième et quatrième catégories sont plus attentatoires à la vie privée que les deux autres. Les accès à ces données sont moins nombreux que ceux aux données d'identification mais restent fréquents. Ces données devront être conservées [9 /12] mois.

9. Versterking van de garanties op het niveau van

9. Le renforcement des garanties au niveau de

de toegang van de overheden tot de gegevens

De EU-richtlijn werd als bijzonder problematisch beschouwd omdat enkel de bewaarplicht erin werd geregeld zonder de toegang van de overheden tot de betrokken gegevens te reglementeren en dus te begeleiden. Het Grondwettelijk Hof merkt het volgende op: "Ook al worden de autoriteiten die gemachtigd zijn tot toegang tot de bewaarde gegevens, opgesomd in artikel 126, § 5, 3°, van de wet van 13 juni 2005, vervangen bij artikel 5 van de bestreden wet, toch wordt bij de wet geen enkele materiële of procedurele voorwaarde vastgelegd met betrekking tot die toegang."

In het vernietigde artikel 126 WEC werd, voor de twee voornaamste toegangsregelingen, nochtans uitdrukkelijk verwezen naar de regels inzake die toegang, met andere woorden de artikelen 46bis en 88bis van het Wetboek van strafvordering voor het strafrechtelijke kader en de artikelen 18/6 en 18/7 van de wet houdende regeling van de inlichtingen- en veiligheidsdienst voor de toegangen op het niveau van de inlichtingenactiviteit.

Dit ontwerp van wet geeft gevolg aan dit deel van het arrest van het Grondwettelijk Hof door het verband tussen artikel 126 WEC en de in de andere voornoemde wetten bepaalde toegangsregeling te versterken. Het verduidelijkt ook het gegeven dat de toegang tot de bewaarde gegevens enkel mogelijk is voor de in artikel 126 WEC uitdrukkelijk vermelde doeleinden.

Dit ontwerp van wet gaat evenwel verder door de garanties waarin is voorzien in het Wetboek van strafvordering en de wet houdende regeling van de inlichtingen- en veiligheidsdienst te versterken. In het ontwerp van wet wordt ook de toegang voor de andere doeleinden beter begeleid. Zij worden verduidelijkt en uitgebreid tot bepaalde zeer specifieke situaties.

a) Versterking van de garanties in het Wetboek van strafvordering

Het ontwerp van wet wijzigt in eerste instantie de regels inzake de toegang tot de

l'accès des autorités aux données

La directive UE a été considérée comme particulièrement problématique parce qu'elle ne réglait que l'obligation de conservation sans réglementer et donc sans encadrer l'accès des autorités aux données concernées. La Cour constitutionnelle note que « si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3°, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès. »

L'article 126 LCE annulé renvoyait pourtant explicitement, pour les deux régimes d'accès principaux, aux règles régissant cet accès, c'est-à-dire les articles 46bis et 88bis du Code d'instruction criminelle pour le cadre pénal et les articles 18/6 et 18/7 de la Loi organique des services de renseignement et de sécurité pour les accès au niveau de l'activité de renseignement.

Le présent projet de loi donne suite à cette partie de l'arrêt de la Cour constitutionnelle en renforçant le lien entre l'article 126 LCE et le régime d'accès défini dans les autres lois précitées. Il clarifie aussi le fait que l'accès aux données conservées n'est possible que pour les finalités explicitement énumérées dans l'article 126 LCE.

Mais le présent projet de loi va plus loin en renforçant les garanties prévues par le Code d'instruction criminelle et la Loi organique des services de renseignement et de sécurité. Il encadre aussi mieux l'accès pour les autres finalités. Celles-ci sont précisées et étendues à certaines situations très spécifiques.

a) Renforcement des garanties dans le Code d'instruction criminelle

Le projet de loi modifie en première instance les règles quant à l'accès aux données d'identification

identificatiegegevens die wordt geregeld in artikel 46bis van het Wetboek van strafvordering en die betrekking heeft op de toegang tot de gegevens van de eerste twee categorieën. Dat artikel 46bis werd reeds gewijzigd door de wetten van 27 december 2004 en van 23 januari 2007. Het is niet mogelijk de procedure te verzwaren voor zo een frequent genomen maatregel en waarvan de impact op de persoonlijke levenssfeer beperkt blijft. De voorwaarden blijven uiteraard van toepassing, inzonderheid de voorafgaande en gemotiveerde instemming van het parket of van de onderzoeksrechter.

qui est réglé par l'article 46bis du Code d'instruction criminelle et qui concerne l'accès aux données des deux premières catégories. Cet article 46bis a déjà été modifié par les lois du 27 décembre 2004 et du 23 janvier 2007. Il n'est pas possible d'alourdir la procédure pour une mesure aussi fréquente et dont l'impact sur la vie privée reste limité. Les conditions restent bien entendu applicables, notamment l'autorisation préalable et motivée du parquet ou du juge d'instruction.

Het ontwerp voert in artikel 46bis niettemin een differentiatie van de toegang tot de gegevens in, door in § 1 toe te voegen dat voor kleinere misdrijven, die gestraft kunnen worden met een correctionele hoofdgevangenisstraf van minder dan een jaar, de gegevens slechts opgevraagd kunnen worden voor een periode van zes maanden voorafgaand aan de beslissing van de procureur des Konings.

Le projet introduit néanmoins une différenciation de l'accès aux donnés à l'article 46bis, en ajoutant au § 1er que pour des infractions de moindre gravité, qui peuvent donner lieu à une peine d'emprisonnement correctionnel principal de moins d'un an, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

De regeling die van toepassing is voor het doen opsporen van de communicaties en dus de toegang tot de gegevens van de laatste twee categorieën wordt ook aanzienlijk versterkt op het stuk van de garanties. Die regeling wordt bepaald in artikel 88bis van het Wetboek van strafvordering. Het ontwerp van wet brengt drie hoofdgaranties aan.

Le régime applicable pour ce qui concerne le repérage des communications et donc l'accès aux données des deux dernières catégories est également considérablement renforcé sur le plan des garanties. Ce régime est défini à l'article 88bis du Code d'instruction criminelle. Le projet de loi apporte trois garanties principales.

Het voert een subsidiariteitsvereiste in: de maatregel kan enkel worden toegestaan als het resultaat niet kan worden behaald door een andere minder indringende maatregel.

Il introduit une exigence de subsidiarité : la mesure ne peut être autorisée que si le résultat ne peut pas être atteint par une autre mesure moins intrusive.

Het ontwerp voert ook een differentiatie in op grond van de ernst van het misdrijf. De maatregel zal niet langer beschikbaar zijn in het kader van de vervolging van misdrijven die worden gestraft met minder dan een jaar gevangenisstraf. Voor de misdrijven die worden gestraft met een gevangenisstraf tot vijf jaar kan de maatregel worden toegestaan maar kan die enkel betrekking hebben op de gegevens met betrekking tot de laatste zes maanden. Voor de misdrijven die worden gestraft met meer dan vijf jaar gevangenisstraf of die zijn opgenomen op de lijst waarin is voorzien in artikel 90ter van het Wetboek van strafvordering (met andere woorden de

Le projet introduit aussi une différenciation sur base de la gravité de l'infraction. La mesure ne sera plus disponible dans le cadre de la poursuite d'infractions punies de moins d'un an d'emprisonnement. Pour les infractions punies de un à cinq ans d'emprisonnement, la mesure pourra être autorisée mais ne pourra porter que sur les données relatives aux six derniers mois. Pour les infractions punies de plus de 5 ans d'emprisonnement ou reprises sur la liste prévue à l'article 90ter du Code d'instruction criminelle (c'est-à-dire les infractions pouvant donner lieu à écoute téléphonique), ou qui sont commises dans le cadre d'une organisation criminelle, la mesure

misdrijven die aanleiding kunnen geven tot telefoontap), of die gepleegd zijn in het kader van een criminele organisatie, kan de maatregel betrekking hebben op de volledige bewaarperiode.

pourra porter sur l'entièreté de la période de conservation.

Ten slotte is voorzien in een uitdrukkelijke bescherming voor de advocaten en de geneesheren.

Enfin, une protection explicite est prévue pour les avocats et les médecins.

b) Versterking van de garanties in de wet houdende regeling van de inlichtingen- en veiligheidsdienst

b) Renforcement des garanties dans la Loi organique des services de renseignement et de sécurité

De toegang tot de bewaarde gegevens wordt geregeld in de artikelen 18/3, 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst. Die toegang wordt reeds grondig begeleid.

L'accès aux données conservées est réglé par les articles 18/3, 18/7 et 18/8 de La loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet accès est déjà fortement encadré.

Artikel 18/3 regelt de procedure voor de aanwending van de specifieke methoden en de controle erop door de onafhankelijke commissie (BIM-commissie). Het artikel strekt eveneens ertoe te voorzien in garanties met het oog op de vrijwaring van het beroepsgeheim van de advocaten en artsen en het bronnengeheim van de journalisten.

L'article 18/3 règle la procédure de mise en œuvre des méthodes spécifiques et leur contrôle par la Commission indépendante, composée de trois magistrats (Commission BIM). Il vise aussi à instaurer des garanties en vue de préserver le secret professionnel des avocats et médecins et le secret des sources des journalistes.

Overeenkomstig artikel 18/3, § 1, van de wet houdende regeling van de inlichtingen- en veiligheidsdienst, kunnen de specifieke methoden slechts worden aangewend indien:

- de gewone methoden ontoereikend blijken om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen (subsidiariteit);
- er een potentiële bedreiging is;
- zij in verhouding staan tot de graad van ernst van de bedreiging;
- de beslissing van het diensthoofd schriftelijk en met redenen omkleed is.

Conformément à l'art. 18/3, §1er de la loi organique, les méthodes spécifiques ne peuvent être mises en œuvre que si :

- les méthodes ordinaires s'avèrent insuffisantes pour récolter les informations nécessaires à une mission de renseignement (subsidiarité) ;
- il y a une menace potentielle ;
- elles sont proportionnelles au degré de gravité de la menace ;
- la décision du chef du service est écrite et motivée.

Die voorwaarden impliceren dat de inlichtingendiensten voor elke methode het verband tussen het doel en de bedreiging moeten aantonen.

Ces conditions impliquent que les services de renseignement doivent, pour chaque méthode justifier le lien entre la cible et la menace.

Geen enkele specifieke methode mag worden aangewend vóór de kennisgeving van de beslissing van het diensthoofd aan de commissie. De wettelijkheid van de specifieke methoden, daaronder begrepen de naleving van de principes van subsidiariteit en proportionaliteit, kan op elk ogenblik worden gecontroleerd door de leden van de commissie. Het Comité I vervult als parlementair controleorgaan een rechtsprekende functie in het kader van de BIM-methoden.

Aucune méthode spécifique ne peut être mise en œuvre avant la notification de la décision du chef du service à la Commission. Le contrôle de légalité des méthodes spécifiques par les membres de la commission, en ce compris le respect de la subsidiarité et de la proportionnalité, peut s'effectuer à tout moment. Le Comité R, organe de contrôle parlementaire, remplit un rôle juridictionnel dans le cadre des méthodes BIM.

Het is voor de inlichtingendiensten verboden om gegevens die worden beschermd door dat beroeps- en bronnengeheim, te verkrijgen, te analyseren of te exploiteren behalve indien de dienst vooraf beschikt over ernstige aanwijzingen dat de advocaat, arts of journalist persoonlijk en actief meewerkt aan een dreiging.

Il est interdit aux services de renseignement d'obtenir, d'analyser et d'exploiter des données protégées par le secret professionnel et le secret des sources si le service dispose au préalable d'indices sérieux selon lesquels l'avocat, le médecin ou le journaliste prend personnellement et activement part à une menace.

In dit geval zijn er drie garanties ingebouwd:

- de methode mag enkel aangewend worden nadat de commissie een eensluidend advies uitgebracht heeft;
- de methode mag niet uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de OVB, van de OBFG, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten hiervan vooraf op de hoogte is.
- de voorzitter van de commissie moet nagaan of de via deze methode verkregen gegevens een rechtstreeks verband hebben met de bedreiging.

Dans ce cas, trois garanties sont intégrées :

- la méthode ne peut être utilisée qu'après que la commission a émis un avis conforme ;
- la méthode ne peut être appliquée sans que, selon le cas, le président de l'OVB, de l'OBFG, du Conseil National de l'Ordre des Médecins ou de l'Association Générale des Journalistes Professionnels en ait été informé au préalable.
- le président de la commission doit vérifier si les données obtenues via cette méthode ont un lien direct avec la menace.

De versterking van de garanties waarin is voorzien in artikel 18/3 strekt hoofdzakelijk tot het verplicht maken van de verschillende vermeldingen en motiveringen in de beslissing van het diensthoofd, waaronder de motivering van de periode van de terugwerkende kracht van de aan de operatoren gevraagde gegevens.

Le renforcement des garanties prévues à l'article 18/3 vise principalement à rendre obligatoire différentes mentions et motivations dans la décision du chef du service, dont la motivation de la période de rétroactivité des données demandées aux opérateurs.

Om de bestaande garanties te versterken wordt ook verduidelijkt dat het diensthoofd verplicht is de methode te beëindigen zodra een illegaliteit wordt vastgesteld, de bedreiging die de methode

Il est également précisé, pour renforcer les garanties existantes, l'obligation pour le dirigeant du service de mettre fin à la méthode dès qu'il est constaté une illégalité, ou que la menace qui l'a

verantwoordde niet meer bestaat of de methode niet langer nuttig is.

c) Voor de andere toegangen

Het ontwerp van wet heeft net zoals de vernietigde wet voornamelijk betrekking op de bewaring met het oog op het strafonderzoek en met het oog op inlichtingen maar andere secundaire doeleinden zijn erin voorzien. Het ontwerp van wet voegt bepaalde gerichte doeleinden toe maar voorziet in belangrijke beperkingen.

Zo zal de cel "Vermiste Personen" van de politie toegang krijgen tot de gegevens in het kader van een onrustwekkende verdwijning maar enkel voor een periode van 48 uur met dien verstande dat een ruimere toegang in het kader van het gerechtelijk onderzoek mogelijk is.

De spoeddiensten die ter plaatse hulp bieden, kunnen in bepaalde situaties bepaalde bewaarde gegevens verkrijgen, voor zover de aanvraag ten aanzien van de operator ten laatste binnen 24 uur na de oproep wordt gedaan.

Voor wat een kwaadwillig gebruik van een elektronisch communicatienetwerk of elektronische communicatiedienst betreft, kan de Ombudsdienst voor Telecommunicatie de identificatiegegevens verkrijgen van de persoon die aan de oorsprong ligt van dat kwaadwillig gebruik, voor zover de aanvraag binnen acht dagen na dat kwaadwillig gebruik wordt gedaan.

10. Versterking van de beveiliging van de door de operatoren bewaarde gegevens

Inzonderheid naar aanleiding van de bekommernissen geuit door het Hof van Justitie versterkt het ontwerp van wet ten slotte de maatregelen die moeten worden genomen door de operatoren en aanbieders om de gegevens en de toegang ertoe te bescherming en te beveiligen. Het gaat inzonderheid erom technologische beschermingsmaatregelen te nemen ten aanzien van die gegevens, de traceerbaarheid van de toegangen te waarborgen, de gegevens te

justifiée n'existe plus, ou qu'elle n'est plus utile.

c) Pour les autres accès

Le projet de loi comme la loi annulée concerne principalement la conservation aux fins de l'enquête pénale ainsi que du renseignement mais d'autres finalités secondaires sont prévues. Le projet de loi ajoute certaines finalités ciblées mais prévoit des limitations importantes.

Ainsi, la cellule « personnes disparues » de la Police aura accès aux données dans le cadre d'une disparition inquiétante mais seulement pour une période de 48 heures étant entendu qu'un accès plus large dans le cadre de l'enquête judiciaire est possible.

Les services d'urgence offrant de l'aide sur place pourront obtenir certaines données conservées dans certaines situations mais pour autant que la demande envers l'opérateur intervienne au plus tard dans les 24 heures de l'appel.

Quant au Service de médiation pour les télécommunications, pour ce qui concerne une utilisation malveillante d'un réseau ou d'un service de communications électroniques, il pourra obtenir les données d'identification de la personne qui est à l'origine de cette utilisation malveillante pour autant que la demande intervienne dans les 8 jours de cette utilisation malveillante.

10. Le renforcement de la sécurisation des données conservées par les opérateurs

Enfin, le projet de loi, faisant suite notamment aux préoccupations émises par la Cour de justice, renforce les mesures à prendre par les opérateurs et fournisseurs de manière à protéger et sécuriser les données et l'accès à celles-ci. Il s'agit notamment de prendre des mesures de protection technologiques à l'égard de ces données, d'assurer la traçabilité des accès, de détruire les données à l'expiration du délai, ou encore de désigner un préposé à la protection des données chargé de

vernietigen na het verstrijken van de termijn, of nog een aangestelde voor de gegevensbescherming aan te wijzen die moet toezien op de inachtneming van de verschillende regels ter zake.

veiller au respect des différentes règles en la matière.

11. Situatie in de andere lidstaten

Een samenvatting van de situatie in de volgende landen zal later worden toegevoegd. Het gaat om de volgende landen: Frankrijk, Verenigd Koninkrijk, Luxemburg, Duitsland, Oostenrijk, Nederland, Denemarken en Zweden.

Hieruit kan worden geconcludeerd dat het beginsel van de bewaring van de gegevens opnieuw in twijfel werd getrokken in Duitsland, Nederland en Oostenrijk maar dat de Duitse en Nederlandse regeringen reeds een ontwerp van wet hebben goedgekeurd op grond waarvan het beginsel opnieuw wordt ingevoerd. De vijf andere staten hebben het beginsel in hun nationale recht behouden. De meeste van die staten hebben geen wijziging aangebracht naar aanleiding van het arrest van het Hof van Justitie van de EU, aangezien zij van oordeel zijn dat dat nationale recht, in zijn geheel genomen en dus met inbegrip van bijvoorbeeld de begeleiding van de toegangen, niet in strijd is met de rechtspraak van de EU. Het Verenigd Koninkrijk heeft zijn regelgeving, naar aanleiding van de vernietiging van de richtlijn, verplaatst in een tekst die kracht van wet heeft. Enkel Luxemburg heeft zijn wetgeving op bepaalde punten aangepast.

11. La situation dans les autres Etats membres

Un résumé de la situation dans les pays suivants sera joint ultérieurement. Il concerne les pays suivants : France, Royaume-Uni, Luxembourg, Allemagne, Autriche, Pays-Bas, Danemark et Suède.

On peut en conclure que le principe de la conservation des données a été remis en cause en Allemagne, aux Pays-Bas et en Autriche mais que les gouvernements allemands et néerlandais ont d'ores et déjà adopté un projet de loi réintroduisant le principe. Les 5 autres Etats ont maintenu le principe dans leur droit national. Parmi ces Etats, la plupart n'a pas apporté de modification suite à l'arrêt de la Cour de justice UE, estimant que, pris dans son ensemble et donc y compris par exemple l'encadrement des accès, ce droit national n'est pas contraire à la jurisprudence UE. Le Royaume-Uni a déplacé, suite à l'annulation de la directive, sa réglementation dans un texte ayant force de loi. Seul le Luxembourg a entrepris l'adaptation de sa législation sur certains points.

ARTIKELSGEWIJZE BESPREKING	**COMMENTAIRES DES ARTICLES**
HOOFDSTUK 1. – Algemene bepaling	**CHAPITRE 1er – Dispositions**
Artikel 1	**Article 1er**
Artikel 1 verwijst naar de grondwettelijke bevoegdheidsverdeling.	L'article 1er renvoie à la répartition constitutionnelle des compétences.
HOOFDSTUK 2. - Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie	**CHAPITRE 2. – Modifications de la loi du 13 juin 2005 relative aux communications électroniques**
Art. 2.	**Art. 2.**
Dit artikel vervangt de definitie van het begrip	Cet article remplace la définition de la notion

"operator" in artikel 2, 11°, van de WEC.

De huidige definitie van het begrip “operator” is niet aanvaardbaar in de praktijk omdat ze een achterpoortje openlaat, in die zin dat personen die geen kennisgeving zouden doen aan het Belgisch Instituut voor postdiensten en telecommunicatie (hierna het BIPT), terwijl ze daartoe verplicht zijn krachtens artikel 9, § 1, van de voormelde wet, niet zouden worden onderworpen aan deze wet. Met de nieuwe definitie van operator kunnen personen die zouden hebben verzuimd aan het BIPT een aangifte te doen als operator, niet langer van dat achterpoortje gebruikmaken: zij moeten de verplichtingen vervullen, zelfs zonder kennisgeving aan het BIPT te hebben gedaan.

Het artikel voegt de definitie van "oproeppoging zonder resultaat" toe in de wet, omdat deze term wordt gebruikt in artikel 126, zoals vervangen door de onderhavige wet. Omdat een spambericht geen bidirectioneel spraakbericht is, vormt dit dus geen oproep, en kan dit dus a fortiori geen oproeppoging zonder resultaat zijn. Spamberichten moeten maar worden bewaard als ze terechtgekomen zijn in de mailbox van de eindgebruiker, onder gelijk welke rubriek. Dit zal de operatoren ertoe aansporen om de antispamfilters te verbeteren.

Art. 3.

Het voorontwerp van wet heft paragraaf 2 van artikel 125 van de WEC op. In werkelijkheid wordt deze paragraaf herschreven, in duidelijker bewoording, in het nieuwe artikel 126/1, § 4, 6°.

Op dit ogenblik wordt de delegatie aan de Koning, waarvan sprake in artikel 125, § 2, ten uitvoer gelegd door het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie. De opheffing van paragraaf 2 van artikel 125 is echter niet problematisch, omdat dit koninklijk besluit al een voldoende wettelijke grondslag heeft, wat de onderhavige wet betreft, in artikel 127, § 1.

Art. 4.

1. Inleiding

d’“opérateur” à l’article 2, 11°, LCE.

La définition actuelle de la notion d’opérateur n’est pas acceptable dans la pratique car elle offre une échappatoire, en ce sens que les personnes qui n’introduiraient pas de notification à l’Institut belge des services postaux et des télécommunications (ci-après “IBPT”) alors qu’elles ont l’obligation de le faire en vertu de l’article 9, § 1er, de la loi précitée, ne seraient pas soumises à cette loi. Avec la nouvelle définition d’opérateur, les personnes qui auraient omis d’introduire une déclaration à l’IBPT comme opérateurs ne peuvent plus invoquer cette échappatoire: elles doivent respecter les obligations, même en l’absence de notification à l’IBPT.

L’article ajoute la définition d’ « appel infructueux » dans la loi, ce terme étant utilisé dans l’article 126 tel que remplacé par la présente loi. Un spam n’étant pas une communication vocale bidirectionnelle, il ne constitue pas un appel, et ne peut donc a fortiori être un appel infructueux. Les spams ne doivent être conservés que lorsqu’ils sont parvenus dans la boite e-mail de l’utilisateur final, sous quelque rubrique que ce soit. Ceci incitera les opérateurs à améliorer les filtres anti-spams.

Art. 3.

L’avant-projet de loi abroge le paragraphe 2 de l’article 125 de la LCE. En réalité, ce paragraphe est réécrit, en des termes plus clairs, dans le nouvel article 126/1, § 4, 6°.

A l’heure actuelle, la délégation au Roi prévue à l’article 125, § 2, a été exécutée par l’arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques. La suppression du paragraphe 2 de l’article 125 n’est cependant pas problématique, dès lors que cet arrêté royal trouve déjà une base légale suffisante, pour ce qui concerne la présente loi, dans l’article 127, § 1er.

Art. 4.

1. Introduction

Artikel 126 is vervangen door de wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering. Deze wet is vernietigd door het Grondwettelijk Hof in een arrest van 11 juni 2015.

Het onderhavige artikel vervangt opnieuw artikel 126, maar brengt daarin een reeks verbeteringen ten opzichte van de versie van artikel 126 dat nietig is verklaard aan.

De nieuwe versie van artikel 126 wordt genomen op basis van artikel 15.1 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 (de zogenaamde "richtlijn betreffende privacy en elektronische communicatie").

Dit artikel biedt de lidstaten de mogelijkheid om reglementaire maatregelen aan te nemen om gegevens gedurende een beperkte periode te bewaren wanneer zulks gerechtvaardigd is om een van de redenen die in dit artikel worden genoemd.

2. Verband met de algemene wetgeving inzake de bescherming van de persoonlijke levenssfeer

De eerste paragraaf van artikel 126 nieuw zegt dat het van toepassing is onverminderd de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Daarom zijn de aanbieders en operatoren uitdrukkelijk verplicht alle bepalingen van de wet van 8 december 1992 en het bijbehorende uitvoeringsbesluit van 13 februari 2001 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

L'article 126 a été remplacé par la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle. Cette loi a été annulée par la Cour constitutionnelle dans un arrêt du 11 juin 2015.

Le présent article remplace à nouveau l'article 126, en apportant toutefois toute un série d'améliorations par rapport à la version de l'article 126 qui a été annulée.

La nouvelle version de l'article 126 est prise sur base de l'article 15.1 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 (dite "directive vie privée et communications électroniques").

Cet article permet aux États membres d'adopter des mesures réglementaires prévoyant la conservation de données pendant une durée limitée lorsque c'est justifié par un des motifs énumérés dans cet article.

2. Lien avec la législation générale en matière de protection de la vie privée

Le paragraphe premier de l'article 126 nouveau indique qu'il s'applique sans préjudice des dispositions 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.

Dès lors, les fournisseurs et opérateurs sont explicitement tenus de respecter l'ensemble des dispositions de la loi du 8 décembre 1992 et de son arrêté d'exécution du 13 février 2001, 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, sous-traitance, 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

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; dit alles onverminderd een klacht bij de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna CBPL) of een verzoek aan de voorzitter van de rechtbank van eerste aanleg. Het spreekt vanzelf dat de betrokken persoon slechts zijn persoonlijke gegevens kan inkijken en niet de gegevens van andere personen.

et pourra, le cas échéant, les faire rectifier, le tout sans préjudice d'une plainte devant la Commission pour la protection de la vie privée (ci-après CPVP) ou d'une requête devant le Président du Tribunal de Première Instance. Il va de soi que la personne concernée ne peut accéder qu'à ses données personnelles et pas aux données d'autres personnes.

3. De ondernemingen die verplicht zijn tot gegevensbewaring

3. Les entreprises tenues de conserver des données

Artikel 126 is van toepassing op de aanbieders van openbare telefoniediensten, waaronder ook via het internet, van internettoegang, van e-mail via het internet, op de aanbieders van de onderliggende openbare elektronische-communicatie-netwerken, alsook op de operatoren die een van deze diensten of netwerken verstrekken.

L'article 126 s'applique aux fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, aux fournisseurs des réseaux publics de communications électroniques sous-jacents ainsi qu'aux opérateurs fournissant un de ces services ou réseaux.

Allereerst moet worden benadrukt dat dit artikel niet van toepassing is op de aanbieders en doorverkopers in de zin van artikel 9, §§ 5 en 6. De aanbieders en doorverkopers zijn immers geen operator en bieden hun diensten niet echt aan het publiek aan.

Il faut d'abord souligner que cet article ne s'applique pas aux fournisseurs et revendeurs au sens de l'article 9, §§ 5 et 6. Ces fournisseurs et revendeurs ne sont en effet pas des opérateurs et n'offrent pas véritablement au public leurs services.

Paragraaf 1 beoogt bepaalde aanbieders en bepaalde operatoren omdat de e-maildienst via het internet niet in alle gevallen binnen het toepassingsgebied van de definitie van elektronische-communicatiedienst valt (art. 2, 5°, van de wet) omdat deze dienst niet altijd bestaat uit het overbrengen van signalen, maar uit het leveren met behulp van elektronische-communicatienetwerken en -diensten van de overgebrachte inhoud.

Le paragraphe 1er vise certains fournisseurs et certains opérateurs dès lors que le courrier électronique par l'Internet n'entre pas dans tous les cas dans le champ d'application de la définition du service de communications électroniques (art. 2, 5° de la loi), car ce service ne consiste pas dans tous les cas à transmettre des signaux mais à fournir, à l'aide de réseaux et services de communications électroniques, du contenu transmis.

Het ontwerp van wet beoogt de telefonie in het algemeen en niet de vaste telefonie, mobiele telefonie of internettelefonie, zoals dat het geval was in de wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering. Er moet immers rekening worden gehouden met de evolutie op de markt en voorzien worden in begrippen die technologieneutraal zijn.

Le projet de loi vise la téléphonie de manière générale et non la téléphonie fixe, mobile ou par Internet comme c'était le cas dans la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle. Il est en effet nécessaire de tenir compte de l'évolution sur le marché et de prévoir des concepts technologiquement neutres.

4. De te bewaren gegevens en de bewaartermijnen

Paragraaf 1 preciseert dat de gegevens enkel moeten bewaard worden door de betrokken aanbieders en operatoren voor zover deze gegevens werden gegenereerd of behandeld door hen in het kader van de verstrekking van de betrokken communicatiediensten. Wanneer dergelijke gegevens niet worden gegenereerd bij of verwerkt door deze aanbieders of operatoren, is er geen verplichting ze te bewaren.

Paragraaf 3 stelt de categorieën van te bewaren gegevens en de bewaartermijnen vast.

Onder communicatiemiddel moet bijvoorbeeld worden verstaan de telefoon die wordt gebruikt om een oproep te doen.

Het eerste en het tweede lid van paragraaf 3 vermelden "vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst." Onder deze zin moet worden verstaan dat de bewaartermijn evolueert met de tijd. De eerste seconde waarin het gebruik van de dienst mogelijk is, moet aldus worden begrepen als de eerste datum vanaf wanneer communicatie voor de laatste maal mogelijk is via de gebruikte dienst. Hetzelfde geldt voor de tweede seconde enzovoort, totdat het gebruik van de dienst niet meer mogelijk is, d.i. tot het einde van het contract. Dit betekent dus ook dat de gegevens die bewaard zijn vóór de bewaartermijn moeten worden vernietigd, voor zover het gaat om andere gegevens dan die welk bewaard worden tijdens de bewaarperiode (bijvoorbeeld als het factureringsadres verandert met de tijd, moet alleen het factureringsadres dat wordt gebruikt door de eindgebruiker tijdens de bewaarperiode worden bewaard).

5. De overheden die toegang kunnen krijgen tot de bewaarde gegevens

Paragraaf 2 van artikel 126 definieert de overheden die de krachtens artikel 126 bewaarde gegevens kunnen krijgen. In die paragraaf wordt echter geen gewag gemaakt van de overheden die gegevens kunnen krijgen die zijn bewaard krachtens de artikelen 122 en 123.

4. Les données à conserver et les délais de conservation

Le paragraphe 1er précise que les données ne doivent être conservées par les fournisseurs et opérateurs en question que pour autant que ces données soient générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés. Dans les cas où ces données ne sont pas générées ou traitées par ces fournisseurs ou opérateurs, il n'y a pas d'obligation de les conserver.

Le paragraphe 3 fixe les catégories de données à conserver et les délais de conservation.

Par moyen de communication, il faut entendre par exemple le téléphone utilisé pour passer un appel.

Les alinéas 1 et 2 du paragraphe 3 se réfèrent à « la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé. » Il faut comprendre par cette phrase que la période de conservation évolue avec le temps. La première seconde pendant laquelle l'utilisation du service est possible doit ainsi être comprise comme la première date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé. Il en est de même pour la deuxième seconde et ainsi de suite, jusqu'à ce que l'utilisation du service ne soit plus possible, soit à la fin du contrat. Cela signifie donc également que les données conservées avant la période de conservation doivent être détruites, pour autant qu'il s'agisse de données différentes de celles conservées pendant la période de conservation (par exemple si l'adresse de facturation change avec le temps, seule l'adresse de facturation utilisée par l'utilisateur final pendant la période de conservation doit être conservée).

5. Les autorités pouvant accéder aux données conservées

Le paragraphe 2 de l'article 126 définit les autorités qui peuvent obtenir des données conservées en vertu de l'article 126. Il ne se prononce cependant pas sur les autorités pouvant obtenir des données conservées en vertu des articles 122 et 123.

Wat de gerechtelijke autoriteiten betreft, verwijst paragraaf 2 naar de artikelen 46bis en 88bis van het Wetboek van Strafvordering. Wat betreft de concrete nadere regels van de samenwerking tussen de operatoren en aanbieders en de gerechtelijke autoriteiten, is het besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie van toepassing.

Pour ce qui concerne les autorités judiciaires, le paragraphe 2 renvoie aux articles 46bis et 88bis du Code d'instruction criminelle. Concernant les modalités concrètes de la collaboration entre les opérateurs et fournisseurs et les autorités judiciaires, est applicable l'arrêté du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

Wat betreft de inlichtingen- en veiligheidsdiensten verwijst paragraaf 2 naar de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Wat betreft de concrete nadere regels van de samenwerking tussen de operatoren en aanbieders en de inlichtingen- en veiligheidsdiensten, geldt het koninklijk besluit van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie.

Pour ce qui concerne les services de renseignement et de sécurité, le paragraphe 2 renvoie aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Concernant les modalités concrètes de la collaboration entre les opérateurs et fournisseurs et les services de renseignement et de sécurité, est applicable l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité.

Het is bovendien van essentieel belang dat elke officier van gerechtelijke politie van het Instituut toegang kan krijgen tot de bewaarde gegevens, opdat zijn controle van de artikelen 114, 124 en 126 van de WEC concreet kan zijn en uitgevoerd worden met werkelijke gegevens. Het volstaat niet dat deze officiers zich tevreden stellen met verklaringen van de operator of aanbieder, die zou beweren deze of gene bepaling van de wet na te leven, of als uitgangspunt hypothetische voorbeelden nemen.

Il est par ailleurs essentiel que tout officier judiciaire de l'Institut puisse avoir accès aux données conservées, afin que son contrôle des articles 114, 124 et 126 de la LCE puisse être concret et puisse être effectué avec des données réelles. Il est n'est pas suffisant que ces officiers se contentent de déclarations de l'opérateur ou du fournisseur, qui prétendrait respecter telle ou telle disposition de la loi ou prennent comme point de départ des exemples hypothétiques.

Het komt vaak voor dat de nooddiensten die ter plaatse hulp bieden, niet de identificatie krijgen van de beller bij een noodoproep, in tegenstelling tot wat artikel 107, § 2, eerste lid, van de WEC voorschrijft. De "identificatie van de oproeper" wordt gedefinieerd in artikel 2, 57° van de WEC als: "elk gegeven, rechtstreeks of onrechtstreeks beschikbaar, in de netwerken en diensten van een operator, dat het oproepnummer van het eindapparaat, de naam van de abonnee en de plaats waar het eindtoestel zich bevindt op het ogenblik van de oproep bepaalt". Welnu, de naam en voornaam van de abonnee, alsook het adres van installatie van de vaste telefoon ("de plaats waar het eindtoestel zich bevindt op het ogenblik van de oproep" in het kader van de vaste telefonie)

Il arrive fréquemment que les services d'urgence offrant de l'aide sur place n'obtiennent pas l'identification de l'appelant lors d'un appel d'urgence, contrairement à ce que l'article 107, § 2, alinéa 1er, de la LCE, prévoit. L' « identification de l'appelant » est définie dans l'article 2, 57°, de la LCE, comme « toute donnée, disponible directement ou indirectement, dans les réseaux et services d'un opérateur, qui détermine le numéro d'appel du terminal, le nom de l'abonné et l'endroit où le terminal se situe au moment de l'appel ». Or le nom et le prénom de l'abonné ainsi que l'adresse d'installation du téléphone fixe (« l'endroit où le terminal se situe au moment de l'appel » dans le cadre de la téléphonie fixe) sont des données conservées en vertu de l'article 126.

zijn gegevens die worden bewaard krachtens artikel 126. Wanneer de hulpdiensten die ter plaatse hulp bieden, deze gegevens niet ontvangen met behulp van de databank die is ingesteld krachtens artikel 107, § 2, derde lid, zullen ze contact mogen opnemen met de operator of de aanbieder in kwestie en deze gegevens krijgen dankzij de gegevens die op basis van het onderhavige artikel moeten worden bewaard. Paragraaf 2 probeert aldus een pragmatische oplossing te bieden aan de nooddiensten die ter plaatse hulp bieden en die geconfronteerd worden met een verzuim van een operator of van een aanbieder, maar doet geen afbreuk aan de mogelijkheid voor het Instituut om de operator te straffen wegens het niet automatisch overzenden en op het moment van de noodoproep, van de identificatiegegevens van de oproeper, zoals voorgeschreven wordt door artikel 107, § 2, eerste lid. Om ten slotte geen procedures op te leggen die moeilijk verzoenbaar zijn met de dringende aard van de hulp die de hulpdiensten moeten verstrekken, schrijft paragraaf 2 niet voor dat de hulpdiensten de identificatiegegevens van de oproeper die worden bewaard op grond van het onderhavige artikel, schriftelijk moeten aanvragen. Deze paragraaf verplicht de operator of aanbieder echter wel om met deze hulpdiensten een veiligheidsmechanisme overeen te komen om te vermijden dat derden, die misbruik zouden maken van de identiteit van de nooddiensten die ter plaatse hulp bieden, op illegale wijze bewaarde gegevens in handen kunnen krijgen.

Si les services d'urgence offrant de l'aide sur place n'obtiennent pas ces données par le biais de la base de données mise en œuvre en vertu de l'article 107, § 2, alinéa 3, ils pourront prendre contact avec l'opérateur ou le fournisseur concerné et obtenir ces données grâce aux données qui doivent être conservées sur base du présent article. Le paragraphe 2 entend ainsi apporter une solution pragmatique aux services d'urgence offrant de l'aide sur place confrontés à un manquement d'un opérateur ou d'un fournisseur mais ne porte pas préjudice à la possibilité pour l'Institut de sanctionner l'opérateur pour n'avoir pas transmis de manière automatique et au moment de l'appel d'urgence les données d'identification de l'appelant, comme prévu à l'article 107, § 2, alinéa 1er. Finalement, afin de ne pas imposer de procédures difficilement conciliables avec le caractère urgent de l'aide que les services d'urgence doivent apporter, le paragraphe 2 ne prévoit pas que les services d'urgence doivent demander par écrit les données d'identification de l'appelant conservées sur base du présent article. Cependant, ce paragraphe oblige l'opérateur ou le fournisseur de convenir avec ces services d'urgence d'un mécanisme de sécurité afin d'éviter que des tiers, qui usurperaient l'identité des services d'urgence offrant de l'aide sur place, puissent obtenir illégalement des données conservées.

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 is (vlucht, poging tot zelfmoord, enz.). Paragraaf twee bepaalt daarom dat de officier van gerechtelijke politie van de cel Vermiste Personen bepaalde gegevens kan krijgen die worden bewaard door de operator of de aanbieder.

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.

Het wetsontwerp bevat bovendien de mogelijkheid voor de Ombudsdienst voor de telecommunicatie om bepaalde bewaarde gegevens te krijgen, wat reeds was opgenomen in de nietig verklaarde wet.

Le projet de loi reprend par ailleurs la possibilité pour le service de médiation pour les télécommunications d'obtenir certaines données conservées, ce qui était déjà prévu dans la loi annulée.

Paragraaf 2 schrijft ook voor dat de gegevens moeten worden verstrekt op eenvoudig verzoek en vanuit België toegankelijk moeten zijn. Dit betekent geenszins dat de voorwaarden die opgenomen zijn in bijvoorbeeld de artikelen 46bis en 88bis van het Wetboek van Strafvordering, niet moeten worden vervuld. Dit betekent daarentegen dat de aanbieder of de operator die in België communicatiediensten verstrekt, de gegevens moet leveren die worden gevraagd door de Belgische overheden op het Belgische grondgebied, zonder dat zij een rogatoire commissie moeten sturen.

Le paragraphe 2 stipule également que les données doivent être fournies sur simple demande et être accessibles à partir de la Belgique. Cela ne signifie nullement que les conditions prévues par exemple dans les articles 46bis et 88bis du Code d'instruction criminelle ne doivent pas être remplies. Cela signifie par contre que le fournisseur ou l'opérateur qui fournit des services de communication en Belgique doit apporter les données demandées par les autorités belges sur le territoire belge, sans que ces dernières ne doivent adresser une commission rogatoire.

Het wetsontwerp verduidelijkt dat het geen afbreuk doet aan de mogelijkheid voor elke overheid vermeld in paragraaf 2, om voor dezelfde doeleinden en met naleving van de voorwaarden waaraan elke overheid moet voldoen, om toegang te hebben tot de gegevens die worden bewaard krachtens artikel 126, de gegevens te krijgen die worden bewaard overeenkomstig de artikelen 122 en 123.

Le projet de loi précise qu'il ne porte pas préjudice à la possibilité pour chaque autorité mentionnée dans le paragraphe 2 d'obtenir, pour les mêmes finalités et en respectant les conditions que chaque autorité doit respecter pour avoir accès aux données conservées en vertu de l'article 126, les données conservées en application des articles 122 et 123

Paragraaf 2 bepaalt ook: "Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden." Daarbij moet een onderscheid worden gemaakt tussen twee gevallen.

Le paragraphe 2 prévoit également que « Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités. » Il faut à cet égard distinguer deux cas de figure.

Ofwel heeft de operator of de aanbieder een database aangelegd voor de commerciële gegevens en een aparte database voor de gegevens die worden bewaard op grond van artikel 126. In dat geval mag hij de tweede database niet gebruiken voor commerciële doeleinden.

Soit l'opérateur ou le fournisseur a mis en place une base de données pour les données commerciales et une base de données distincte pour les données conservées sur base de l'article 126. Dans ce cas, il ne peut pas utiliser la deuxième base de données pour des fins commerciales.

Ofwel heeft de operator of de aanbieder beslist één enkele database te houden voor de commerciële gegevens die hij mag bewaren krachtens de artikelen 122 en 123 en voor de gegevens die hij moet bewaren op grond van artikel 126. In dat geval zal hij voor de bewaarde gegevens de doeleinden in acht moeten nemen die vastgelegd zijn door de verschillende toepasselijke artikelen (de artikelen 122, 123 en 126). Zo zal een gegeven dat hij moet bewaren op basis van artikel 126, maar niet mag bewaren op basis van de artikelen 122 en 123, niet mogen gebruiken voor commerciële doeleinden.

Soit l'opérateur ou le fournisseur a décidé de maintenir une seule base de données pour les données commerciales qu'il peut conserver en vertu des articles 122 et 123 et pour les données qu'il doit conserver en vertu de l'article 126. Dans ce cas, il devra, pour les données conservées, respecter les finalités prévues par les différents articles applicables (articles 122, 123 et 126). Ainsi, une donnée qu'il doit conserver sur base de l'article 126 mais qu'il ne peut pas conserver sur base des articles 122 et 123 ne peut pas être utilisée à des fins commerciales.

6. De door de operatoren en aanbieders te nemen veiligheids- en beschermingsmaatregelen

Paragraaf 4 gaat over de veiligheids- en beschermingsmaatregelen die de operatoren en leveranciers moeten nemen.

Men moet allereerst voor ogen houden dat het niet gepast is om gegevens die krachtens artikel 126 bewaard moeten worden in een excessieve reglementering te gieten. Er zijn nog andere persoonsgegevens die de operatoren en aanbieders verwerken (en al of niet bewaren) en die ook een hoog niveau van bescherming verdienen. Allereerst moet dus de algemene reglementering inzake bescherming van gegevens worden toegepast die vervat is in de wet en de algemene referentiemaatregelen die ingesteld zijn door het Instituut en de CBPL.

Paragraaf 4 enerzijds neemt, soms in een herwerkte versie, bepaalde veiligheidsmaatregelen over die al in de nietig verklaarde wet stonden. Anderzijds zijn in paragraaf 4 extra maatregelen toegevoegd.

Zo geschiedt de toegang tot de gegevens niet langer via een lid van de Coördinatiecel Justitie van de operator of van de aanbieder maar via een lid van de Coördinatiecel van de operator of van de aanbieder, zoals bedoeld in artikel 126/1, § 1. De wet preciseert zelf de voorwaarden die aan deze leden verbonden zijn, in plaats van te verwijzen naar een koninklijk besluit, zoals voordien het geval was.

Bovendien wordt ook gepreciseerd dat de gegevens moeten worden vernietigd van elke drager na afloop van de bewaartermijn, onverminderd de artikelen 122 en 123. Men kan immers niet uitsluiten dat een aanbieder of operator slechts één databank heeft aangelegd in het kader van de artikelen 122, 123 en 126. In dat geval zal een gegeven niet worden vernietigd op grond van artikel 126 als die nog kan worden bewaard op basis van de artikelen 122 en 123 van de wet.

Paragraaf 4 legt ook de volgende nieuwe veiligheidsmaatregelen op die de operatoren moeten nemen.

6. Les mesures de sécurité et de protection des données à prendre par les opérateurs et fournisseurs

Le paragraphe 4 traite des mesures de sécurité et de protection à prendre par les opérateurs et fournisseurs.

Il faut tout d'abord garder à l'esprit qu'il n'est pas approprié de verser dans une réglementation excessive des données conservées en vertu de l'article 126. Il existe d'autres données à caractère personnel que les opérateurs et fournisseurs traitent (et conservent ou non) et qui méritent également un haut niveau de protection. Il faut donc appliquer tout d'abord la réglementation générale de protection des données contenues dans la loi et les mesures de référence générales mises en place par l'Institut et la CPVP.

Le paragraphe 4 d'une part reprend, en les retravaillant parfois, certaines mesures de sécurité qui existait déjà dans la loi annulée. D'autre part, des mesures supplémentaires ont été rajoutées au paragraphe 4.

Ainsi, l'accès aux données ne se fait plus via un membre de la Cellule coordination de la Justice de l'opérateur ou du fournisseur mais via un membre de la Cellule de coordination de l'opérateur ou du fournisseur telle que visée à l'article 126/1, § 1er. La loi précise elle-même les conditions attachées à ces membres plutôt que de renvoyer vers un arrêté royal comme c'était le cas auparavant.

Par ailleurs, il est également précisé que les données doivent être détruites de tout support à l'issue de la période de conservation, sans préjudice des articles 122 et 123. En effet, on ne peut pas exclure qu'un fournisseur ou opérateur n'ait établi qu'une seule base de données dans le cadre des articles 122, 123 et 126. Dans ce cas, une donnée ne sera pas détruite en vertu de l'article 126 si elle peut encore être conservée sur base des articles 122 et 123 de la loi.

Le paragraphe 4 impose également les nouvelles mesures de sécurité suivantes à prendre par les opérateurs.

Ten eerste wordt bepaald dat de gegevens moeten worden bewaard op het grondgebied van de Europese Unie, om rekening te houden met het arrest van 8 april 2014 van het Hof van Justitie van de Europese Unie.

Ten tweede moeten de aanbieders en operatoren zorgen voor maatregelen van technologische bescherming die de bewaarde gegevens, van bij hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er inzage in te hebben. Deze nieuwe verplichting is geïnspireerd op artikel 4.1 van Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.

Ten derde moet een traceerbaarheid van de exploitatie van de bewaarde gegevens worden ingevoerd met behulp van een journaal. Deze traceerbaarheid vormt een bijkomende garantie voor de aangestelde voor de bescherming van de persoonsgegevens, alsook voor het Instituut en de CBPL om een controle te verrichten op de correcte toepassing van de wet.

7. Evaluatie van de wet

De paragrafen 5 en 6 van artikel 126 voorzien in een dubbele evaluatie van de wet.

Enerzijds moet twee jaar na de inwerkingtreding van het toekomstige koninklijk besluit ter uitvoering van artikel 126, § 3 een eenmalige ruime evaluatie worden doorgevoerd; daarbij zullen de verantwoordelijke ministers verslag uitbrengen aan de Kamer van Volksvertegenwoordigers over de toepassing van de wet, en eventueel zullen inhoudelijke aanbevelingen kunnen worden geformuleerd over de bewaartermijnen, de inhoud van de bewaarde gegevens, de praktische toepassing, enz. Eventueel zou deze evaluatie kunnen leiden tot gepaste initiatieven.

Anderzijds voorziet het wetsontwerp ook in een jaarlijks verslag aan de Kamer van Volksvertegenwoordigers. Het gaat in dit geval eerder om een statistisch rapport, zoals dat al is

Premièrement, il est prévu que les données doivent être conservées sur le territoire de l'Union européenne, pour tenir compte de l'arrêt du 8 avril 2014 de la Cour de Justice de l'Union européenne.

Deuxièmement, les fournisseurs et opérateurs doivent mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, incompréhensibles et inexploitables pour toute personne qui n'est pas autorisé à y avoir accès. Cette nouvelle obligation s'inspire de l'article 4.1. du Règlement (UE) n° 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

Troisièmement, une traçabilité de l'exploitation des données conservées doit être mise en place à l'aide d'un journal. Cette traçabilité constitue une garantie supplémentaire permettant au préposé à la protection des données ainsi qu'à l'Institut et à la CPVP d'effectuer un contrôle sur l'application correcte de la loi.

7. Evaluation de la loi

Les paragraphes 5 et 6 de l'article 126 prévoient une double évaluation de la loi.

D'une part, deux ans après l'entrée en vigueur du futur arrêté royal exécutant l'article 126, § 3, une vaste évaluation unique devra être menée; à cet égard, les ministres responsables feront rapport à la Chambre des représentants sur l'application de la loi, et, éventuellement des recommandations de contenu pourront être formulées concernant les délais de conservation, le contenu des données conservées, l'application pratique, etc. Le cas échéant, cette évaluation pourrait conduire à des initiatives appropriées.

D'autre part, le projet de loi prévoit également un rapport annuel à la Chambre des Représentants. Il s'agit en l'occurrence plutôt d'un rapport statistique, comme cela est déjà prévu pour

voorgeschreven voor sommige onderzoeksmaatregelen in artikel 90decies van het Wetboek van Strafvordering.

certaines mesures d'instruction à l'article 90decies du Code d'instruction criminelle.

8. Terugbetaling van de kosten van de operatoren

8. Remboursement des coûts des opérateurs

Artikel 126 voorziet niet in een compensatiemechanisme voor de kosten van de aanbieders en operatoren voor de inzameling, registratie, bewaring en vernietiging van de gegevens. Deze verrichtingen komen dus ten laste van de aanbieders en operatoren. De kosten voor opslag vertegenwoordigen slechts een heel klein deel van alle kosten waaraan de aanbieders en operatoren worden blootgesteld in het kader van de identificatie en de wettelijke onderschepping. Dankzij de technologische vooruitgang zullen de kosten voor de nodige apparatuur overigens beduidend dalen van jaar tot jaar.

L'article 126 ne prévoit pas de mécanisme de compensation des coûts des fournisseurs et opérateurs pour la récolte, l'enregistrement, la conservation et la destruction des données. Ces opérations sont donc à charge des fournisseurs et opérateurs. Les coûts de stockage ne représentent qu'une très petite partie de l'ensemble des coûts qu'exposent les fournisseurs et les opérateurs dans le cadre de l'identification et de l'interception légale. De plus, grâce au progrès technologique, les coûts de l'équipement nécessaire pour le stockage diminueront sensiblement d'année en année.

Krachtens artikel 46bis en artikel 88bis van het Wetboek van strafvordering worden momenteel daarentegen wel vorderbare vergoedingen genoemd in de bijlage bij het koninklijk besluit van 9 januari 2003 houdende de nadere regels voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie. Dat koninklijk besluit beoogt de communicatie aan de gerechtelijke autoriteiten van zowel de gegevens die worden bewaard krachtens dit wetsontwerp en het besluit tot uitvoering van artikel 126 als de gegevens die niet worden bewaard krachtens deze wetgevingen.

Par contre, des indemnités par réquisition sur la base de l'article 46bis et de l'article 88bis du Code d'instruction criminelle figurent actuellement à l'annexe de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques. Cet arrêté royal vise la communication aux autorités judiciaires tant des données qui sont conservées en vertu du présent projet de loi et de l'arrêté d'exécution de l'article 126 que des données qui ne sont pas conservées en vertu de ces législations.

De voormelde vergoedingen zijn bedoeld als compensatie voor de aanbieders en operatoren van bepaalde kosten inzake de opzoeking van gegevens en communicatie van gegevens aan de gerechtelijke autoriteiten.

Les indemnités susmentionnées visent à rembourser aux fournisseurs et opérateurs certains coûts relatifs à la recherche de données et à la communication de données aux autorités judiciaires.

Art. 4.

Art. 4.

Paragraaf 1 van het nieuwe artikel 126/1 is geïnspireerd op artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.

Le paragraphe 1er du nouvel article 126/1 s'inspire de l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

Krachtens dit artikel 2 moet iedere operator van een elektronische-communicatienetwerk en iedere aanbieder van een elektronische-communicatiedienst een "Coördinatiecel Justitie"

En vertu de cet article 2, chaque opérateur d'un réseau de communications électronique et chaque fournisseur d'un service de communications électroniques doit constituer une " Cellule de

oprichten om te antwoorden op de requisitoirs die genomen zijn op basis van de artikelen 46bis, § 2, 88bis, § 2, en 90quater, § 2, van het Wetboek van Strafvordering. In 2010 is de mogelijkheid gecreëerd voor de inlichtingen- en veiligheidsdiensten om een beroep te doen op deze cel (zie artikel 2, § 1, van het koninklijk besluit van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie). In de praktijk nemen de nooddiensten die ter plaatse hulp bieden ook geregeld contact op met deze cel, om de identificatiegegevens van de oproeper te krijgen, die de operator nalaat automatisch aan hen te verstrekken bij een noodoproep. Gelet op de historische evolutie van de opdrachten van de Coördinatiecel Justitie die zich daarom niet beperkt tot de diensten van Justitie, wordt deze cel de Coördinatiecel.

coordination de la Justice " pour répondre aux réquisitoires pris sur base des articles 46bis, § 2, 88bis, § 2, et 90quater, § 2, du Code d'instruction criminelle. En 2010, la possibilité a été créé pour les services de renseignement et de sécurité de faire appel à cette cellule (voir article 2, § 1er, de l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité). En pratique, les services d'urgence offrant de l'aide sur place contactent également régulièrement cette cellule pour obtenir les données d'identification de l'appelant que l'opérateur est en défaut de leur fournir de manière automatique lors d'un appel d'urgence. Vu l'évolution historique des missions de la Cellule de coordination de la Justice qui ne se limite dès lors pas qu'aux services de la Justice, cette Cellule devient la Cellule de coordination.

Deze Coördinatiecel zal dus worden belast met het verstrekken aan de wettelijk bevoegde overheden, om op hun verzoek onder andere bepaalde gegevens te verstrekken die worden bewaard krachtens artikel 126, maar ook sommige commerciële gegevens die worden bewaard op grond van de artikelen 122 en 123.

Cette Cellule de coordination sera donc chargée de fournir aux autorités belges légalement autorisées, à leur demande, entre autres certaines données conservées en vertu de l'article 126 mais également certaines données commerciales conservées en vertu des articles 122 et 123.

Elk lid van de Coördinatiecel moet het voorwerp hebben uitgemaakt van een positief veiligheidsadvies, dat bestemd is om zijn betrouwbaarheid te garanderen. Deze betrouwbaarheid is belangrijk om twee redenen. Enerzijds zullen deze personen toegang hebben tot gevoelige gegevens die zijn verwerkt door de operator of de aanbieder, en anderzijds zullen deze personen kennis moeten nemen van de aanvragen van de overheden en in het bijzonder van de requisitoirs van de gerechtelijke autoriteiten en van de inlichtingen- en veiligheidsdiensten.

Chaque membre de la Cellule de coordination doit avoir fait l'objet d'un avis de sécurité positif, qui a pour vocation de garantir sa fiabilité. Cette fiabilité est importante pour deux raisons. D'une part, ces personnes auront accès à des données sensibles traitées par l'opérateur ou le fournisseur et, d'autre part, ces personnes seront amenées à prendre connaissance des demandes des autorités et en particulier des réquisitoires des autorités judiciaires et des services de renseignement et de sécurité.

Paragraaf twee van het nieuwe artikel 126/1 neemt verscheidene bestaande bepalingen over. Het eerste lid neemt paragraaf 6 van artikel 127 over, want dit lid hoort eerder thuis in artikel 126/1, dat de gemeenschappelijke regels omvat die van toepassing zijn op de samenwerking van de operatoren en van de aanbieders met de overheden voor de verstrekking van de identificatie-, verkeers- of inhoudelijke gegevens.

La paragraphe deux du nouvel article 126/1 reprend plusieurs dispositions existantes. L'alinéa 1er reprend le paragraphe 6 de l'article 127, car cet alinéa a plus sa place dans l'article 126/1, qui comprend les règles communes applicables à la collaboration des opérateurs et des fournisseurs avec les autorités pour la fourniture des données d'identification, de trafic ou de contenu.

Het tweede lid neemt paragraaf 5, derde lid, over van het nietig verklaarde artikel 126.

Het derde lid wordt verklaard door het feit dat artikel 114, § 2, enkel van toepassing is op "ondernemingen die algemeen beschikbare elektronische-communicatiediensten verstrekken". Welnu, de verplichting om gegevens te bewaren krachtens artikel 126 weegt ook op de aanbieders van algemeen beschikbare telefoniediensten, inclusief via het internet, van internettoegang, van e-mail via het internet en op de aanbieders van openbare elektronische-communicatienetwerken.

Paragraaf 3 van het nieuwe artikel 126/1 is geïnspireerd op artikel 8 van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie. De functie van de aangestelde voor de bescherming van de persoonsgegevens wordt uitgebreid tot de gegevens die commercieel worden bewaard omdat de operator of de aanbieder kan hebben beslist om één enkele database te houden voor de commerciële gegevens die hij mag bewaren krachtens de artikelen 122 en 123 en voor de gegevens die hij moet bewaren op grond van artikel 126. In dat geval zal hij voor de bewaarde gegevens de respectieve doeleinden in acht moeten nemen die vastgelegd zijn door de verschillende toepasselijke artikelen (de artikelen 122, 123 en 126). Een controle van de naleving van de respectieve doeleinden door een aangestelde voor de bescherming van de gegevens is dus noodzakelijk.

De aangestelde beschikt over een statuut en een mandaat dat onder andere de mogelijkheid biedt om een controle uit te oefenen op de conformiteit van de verwerkingen van de bewaarde gegevens met de onderhavige wet, zowel ten aanzien van de operator of de aanbieder in het algemeen, als ten aanzien van de Coördinatiecel in het bijzonder. Hij moet toegang hebben tot de gegevens die worden bewaard krachtens de artikelen 122, 123 en 126 en hij moet zijn mandaat in volle onafhankelijkheid kunnen uitoefenen. Om zijn positie te versterken is daarom beslist - in tegenstelling tot de nietig verklaarde wet - dat de aangestelde geen deel uitmaakt van de Coördinatiecel. Hij moet immers in volle onafhankelijkheid en onpartijdig de werking van de Cel kunnen controleren.

L'alinéa 2 reprend le paragraphe 5, alinéa 3, de l'article 126 annulé.

L'alinéa 3 s'explique par le fait que l'article 114, § 2, n'est applicable que pour « les entreprises fournissant des services de communications électroniques accessibles au public ». Or l'obligation de conserver des données en vertu de l'article 126 repose également sur les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet et sur les fournisseurs des réseaux publics de communications électroniques.

Le paragraphe 3 du nouvel article 126/1 s'inspire de l'article 8 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. La fonction du préposé à la protection des données à caractère personnel est étendue aux données conservées à titre commercial, dès lors que l'opérateur ou le fournisseur peut avoir décidé de maintenir une seule base de données pour les données commerciales qu'il peut conserver en vertu des articles 122 et 123 et pour les données qu'il doit conserver en vertu de l'article 126. Dans ce cas, il devra, pour les données conservées, respecter les finalités respectives prévues par les différents articles applicables (articles 122, 123 et 126). Un contrôle du respect des finalités respectives par un prépose à la protection des données s'impose donc.

Le préposé dispose d'un statut et d'un mandat permettant, entre autres, d'effectuer un contrôle de la conformité des traitements des données conservées avec la présente loi tant à l'égard de l'opérateur ou le fournisseur en général qu'à l'égard de la Cellule de coordination en particulier. Il doit avoir accès aux données conservées en vertu des articles 122, 123 et 126 et il doit pouvoir effectuer son mandat en toute indépendance. Afin de renforcer sa position il a donc été décidé – contrairement à la loi annulée – que le préposé ne fasse pas partie de la Cellule de coordination. En effet, il doit pouvoir contrôler en toute indépendance et impartialement le fonctionnement de la Cellule.

Paragraaf 4 van het nieuwe artikel 126/1 voorziet in een reeks delegaties aan de Koning. De punten 1° en 4° moeten de Koning in staat stellen om regels vast te stellen die aangepast zijn voor de operatoren of aanbieders die in het buitenland gevestigd zijn of die maar weinig of geen verzoeken van de overheden inzake identificatie-, verkeers- of inhoudelijke gegevens ontvangen. Punt 6° is geïnspireerd op paragraaf 2 van artikel 125, dat door de onderhavige wet wordt opgeheven.

Le paragraphe 4 du nouvel article 126/1 prévoit une série de délégations au Roi. Les points 1° et 4° doivent permettre au Roi de prévoir des règles adaptées pour les opérateurs ou fournisseurs qui sont établis à l'étranger ou qui ne reçoivent que peu ou jamais de demandes des autorités en matière de données d'identification, de trafic ou de contenu. Le point 6° s'inspire du paragraphe 2 de l'article 125 que la présente loi abroge.

Art. 5.

Art. 5.

De wijzigingen in de eerste paragraaf van artikel 127 zijn nodig om het persoonlijke toepassingsgebied van artikel 126 te weerspiegelen.

Les modifications au paragraphe premier de l'article 127 sont nécessaires pour refléter le champ d'application personnel de l'article 126.

Paragraaf 6 is verplaatst in paragraaf 2 van het nieuwe artikel 126/1.

Le paragraphe 6 a été déplacé dans le paragraphe 2 du nouvel article 126/1.

Art. 6.

Art. 6.

Artikel 126 wordt toegevoegd aan de lijst waarvan sprake in artikel 145, § 1, omdat de door de operatoren en aanbieders krachtens artikel 126 bewaarde gegevens, worden bewaard in het belang van de maatschappij.

L'article 126 est ajouté dans la liste prévue à l'article 145, § 1er, parce que les données conservées par les opérateurs et les fournisseurs en vertu de l'article 126 le sont dans l'intérêt de la société.

Artikel 126/1 wordt toegevoegd aan de lijst waarvan sprake in artikel 145, § 1, omdat het sommige bepalingen overneemt van artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie. Welnu, dit koninklijk besluit is onder meer genomen op grond van artikel 127, dat reeds in de lijst staat die vastgesteld is in artikel 145, § 1.

L'articles 126/1 est ajouté dans la liste prévue à l'article 145, § 1er, parce qu'il reprend certaines dispositions de l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques. Or cet arrêté royal est pris entre autres sur base de l'article 127, qui se trouve déjà dans la liste fixée à l'article 145, § 1er.

Art. 7.

Het wetsontwerp voegt een bijkomende strafbepaling in, die de reeds bestaande strafbepalingen in het Strafwetboek aanvult in verband met externe en interne hacking.

Art. 7.

Le projet de loi insère une disposition pénale additionnelle, complétant les dispositions pénales déjà existantes dans le Code pénal concernant le hacking externe et interne.

Het doel van het artikel is de vertrouwelijkheid van de gegevens te beschermen en de toegang tot, het bezit en het gebruik van deze gegevens overeenkomstig de wettelijk bepaalde doeleinden te garanderen.

Le but de l'article est de protéger la confidentialité des données et garantir l'accès à, la possession et l'utilisation de ces données conformément aux finalités légalement prévues.

Er moeten evenwel geen nieuwe incriminaties gecreëerd worden voor daden die reeds door andere strafbepalingen gedekt worden. Dit zou enkel nuttig zijn indien men van mening is dat de bestaande strafbepalingen niet voldoende zijn.

Cependant, il ne faut pas créer de nouvelles incriminations pour des actes qui sont déjà couverts par d'autres dispositions pénales. Il serait utile de le faire seulement si l'on estime que les dispositions pénales existantes ne sont pas suffisantes.

Het is dus noodzakelijk om verschillende gevallen te onderscheiden en te kijken welke de bestaande bepalingen zijn die erop van toepassing kunnen zijn, om slechts een nieuw strafbaar feit te creëren voor de gevallen die nog niet gedekt zijn. Wanneer een persoon niet gemachtigd is om toegang te hebben tot het systeem en er zich toch toegang toe verschaft, kan er verwezen worden naar artikel 550bis, § 1, van het Strafwetboek: externe hacking, met verzwarende omstandigheden in geval van bezit, onthulling, verspreiding of gebruik van de gegevens (§§ 3 en 7).

Il est donc nécessaire de distinguer différents cas de figure et de voir quelles sont les dispositions existantes qui pourraient s'y appliquer afin de ne créer une nouvelle infraction que pour ce qui n'est pas encore couvert. Lorsqu'une personne qui n'est pas autorisée à accéder au système y accède quand même, nous renvoyons ici à l'article 550bis, § 1er, du Code pénal: le hacking externe, avec les circonstances aggravantes en cas de détention, divulgation, distribution ou usage des données (§§ 3 et 7).

Wanneer een persoon gemachtigd is om toegang te hebben tot het systeem en zijn toegangsbevoegdheid overschrijdt, kan er verwezen worden naar de interne hacking (artikel 550bis, § 2, van het Strafwetboek en §§ 3 en 7). Dit zal bijvoorbeeld het geval zijn voor de persoon die werkt in de Coördinatiecel bedoeld in artikel 126/1, maar zich toegang verschaft tot de gegevens zonder gerechtelijke vordering. Niettemin, wanneer de persoon zijn toegangsbevoegdheid niet overschrijdt, maar later onwettig gebruikmaakt van de gegevens die hij op een wettelijke en gerechtvaardigde manier uit het systeem heeft gehaald, is deze hypothese niet gedekt door de wet.

Lorsqu'une personne est autorisée à accéder au système et outrepasse son pouvoir d'accès, il peut être renvoyé au hacking interne (article 550bis, § 2 Code pénal et §§ 3 et 7). Ce sera, par exemple, le cas de la personne qui travaille à la Cellule coordination visée à l'article 126/1, § 1er, mais qui accède aux données en dehors de toute requête judiciaire. Néanmoins, lorsqu'elle n'outrepasse pas son pouvoir d'accès, mais fait ultérieurement un usage non autorisé par la loi des données qu'elle a extraites du système d'une manière légale et justifiée, cette hypothèse n'est pas couverte par la loi.

Dit is dan ook de reden waarom in artikel 145, § 3ter, van de wet een nieuwe incriminatie ingevoegd wordt die de elementen overneemt die nog niet gedekt zijn door de artikelen van het Strafwetboek.

C'est la raison pour laquelle on introduit dans l'article 145, §3ter, de la loi une nouvelle incrimination qui reprend les éléments qui ne sont pas encore couverts par les articles du Code pénal.

De nieuwe strafsancties ingevoerd door artikel 7 doen geen afbreuk aan de andere sancties die reeds van toepassing zijn.

Les nouvelles sanctions pénales introduites par l'article 7 laissent intactes les autres sanctions déjà en vigueur.

Wat dat betreft, voorziet artikel 39 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in een boete van 100 tot 100.000 EUR volgens de huidige van kracht zijnde wetgeving voor de verantwoordelijke

À cet égard, l'article 39 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 prévoit une amende pénale de 100 à 100 000 EUR selon la législation actuellement en vigueur pour tout responsable de traitement (ou

voor verwerking (of de aangestelde of gevolmachtigde) die artikel 4, § 1, van de voornoemde wet overtreedt, met name de kwaliteit van de gegevens (niet buitensporig veel gegevens, geen oneindige bewaringstermijn, geen oneigenlijk gebruik ten opzichte van de bepaalde doeleinden, enz.).

Artikel 14, 3°, van de wet van 17 januari met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector maakt het Instituut bovendien bevoegd voor de controle op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie en de bijbehorende uitvoeringsbesluiten, en krachtens artikel 21, § 6, van de wet van 17 januari 2003 mag het BIPT een administratieve boete opleggen die voor een overtreder die een omzet behaalt en, in geval van niet-naleving van een eerste besluit van het BIPT waarbij hem een administratieve boete wordt opgelegd, kan gaan tot 10% van het omzetcijfer van de overtreder, dat in de loop van het meest recente boekjaar behaald is in de elektronische-communicatiesector in België.

Het geheel van de voormelde bepalingen impliceert dat niet alleen het BIPT en de CBPL, maar ook de gerechtelijke autoriteiten de goede afloop van de gegevensbewaring mogen controleren.

préposé ou mandataire) qui enfreint l'article 4, § 1er, de ladite loi, à savoir la qualité des données (pas de données excessives, pas de durée de conservation éternelle, pas d'utilisation incompatible avec les finalités prévues, etc.).

L'article 14, § 3, de la loi du 17 janvier 2003 relatif au statut du régulateur des secteurs des postes et des télécommunications belges donne, en outre, la compétence à l'Institut pour contrôler notamment le respect de la loi du 13 juin 2005 relative aux communications électroniques et de ses arrêtés d'exécution, et l'article 21, § 6, de la loi du 17 janvier 2003 permet à l'IBPT d'infliger une amende administrative pouvant aller, pour un contrevenant qui réalise un chiffre d'affaires et, en cas de non-respect d'une première décision de l'IBPT lui imposant une amende administrative, jusqu'à 10 % du chiffre d'affaires du contrevenant réalisé au cours de l'exercice complet le plus récent dans le secteur des communications électroniques en Belgique.

L'ensemble des dispositions précitées implique que non seulement l'IBPT et la CPVP, mais aussi les autorités judiciaires peuvent contrôler le bon déroulement de la conservation des données.

HOOFDSTUK 3. - Bepalingen tot wijziging van het Wetboek van strafvordering

Art. 8

Dit artikel voegt een vierde lid toe aan §1 van artikel 46bis van het Wetboek van strafvordering.

Zoals reeds uitgelegd werd in het algemeen gedeelte van deze memorie van toelichting wordt een differentiatie voor wat betreft de toegang tot de gegevens voorzien in artikel 46bis. Voor lichtere misdrijven, die een correctionele gevangenisstraf van minder dan één jaar tot gevolg kunnen hebben, kunnen de gegevens slechts opgevraagd worden voor een periode van zes maanden voorafgaand aan de beslissing van de procureur des Konings.

Art. 9

Cet article comporte un certain nombre de modifications à l'article 88bis du Code d'instruction criminelle.

CHAPITRE 3. – Dispositions modifiant le Code d'instruction criminelle

Art. 8

Cet article ajoute un alinéa 4 au § 1er de l'article 46bis du Code d'instruction criminelle.

Comme déjà expliqué dans la partie générale de cet exposé des motifs, une différenciation de l'accès aux donnés est introduit à l'article 46bis. Pour des infractions de moindre gravité, qui peuvent donner lieu à une peine d'emprisonnement correctionnel principal de moins d'un an, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

Art. 9

Dit artikel bevat een aantal wijzigingen aan artikel 88bis van het Wetboek van strafvordering.

Dans son arrêt n° 84/2015 du 11 juin 2015, la Cour constitutionnelle a notamment souligné le fait que la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle ne définit aucune condition matérielle ou procédurale en matière d'accès aux données conservées (cf. considérant B.10.3.). La Cour néglige le fait qu'en ce qui concerne les autorités judiciaires, l'accès aux données conservées est régi par le Code d'instruction criminelle, plus particulièrement par les articles 46bis et 88bis, qui définissent les conditions matérielles et procédurales.

In het arrest nr. 84/2015 van 11 juni 2015 heeft het Grondwettelijk Hof onder meer gewezen op het feit dat de wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering, geen enkele materiële of procedurele voorwaarde vastgelegd heeft met betrekking tot de toegang van de bewaarde gegevens (zie overweging B.10.3.). Het Hof ziet daarbij over het hoofd dat de toegang tot de bewaarde gegevens, voor wat betreft de gerechtelijke autoriteiten, geregeld wordt in het Wetboek van strafvordering, meer bepaald in de artikelen 46bis en 88bis, waar de materiële en procedurele voorwaarden vastgelegd zijn.

Afin de répondre aux préoccupations de la Cour, le gouvernement a décidé d'inclure des garanties et des conditions supplémentaires dans l'article 88bis, qui porte sur la demande de données de trafic et de localisation. Ces données sont en effet plus sensibles sur le plan de la vie privée que les données d'identification visées à l'article 46bis en ce sens que, comme le signale la Cour européenne de Justice dans son arrêt du 8 avril 2014, elles permettent de tirer des conclusions précises sur la vie privée des personnes dont les données sont conservées.

Om tegemoet te komen aan de bezorgdheden van het Hof, kiest de Regering er voor om extra garanties en voorwaarden in te schrijven in artikel 88bis, dat betrekking heeft op het opvragen van verkeers- en lokalisatiegegevens. Deze gegevens zijn immers meer privacygevoelig dan de identificatiegegevens bedoeld in artikel 46bis, in die zin dat ze, zoals het Europese Hof van Justitie haar arrest van 8 april 2014 heeft aangestipt, het mogelijk maken om precieze conclusies te trekken over het privéleven van de personen wiens data bewaard worden.

La Cour a également signalé en ce qui concerne la durée de conservation des données qu'aucune distinction n'est opérée entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées (considérant B.10.4.). Une telle distinction entre les catégories de données a déjà été opérée lors de la subdivision en données d'identification visées à l'article 46bis et données de trafic et de localisation visées à l'article 88bis. Ces dernières font de toute manière déjà l'objet de conditions et de procédures plus strictes.

Het Hof heeft er ook op gewezen dat, wat de bewaarperiode van de gegevens betreft, er geen enkel onderscheid gemaakt wordt tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken persoon (overweging B.10.4.). Een dergelijk onderscheid tussen categorieën van gegevens is al gemaakt geworden bij de opdeling van enerzijds de identificatiegegevens bedoeld in artikel 46bis, en anderzijds de verkeers- en lokalisatiegegevens bedoeld in artikel 88bis. Voor die laatste gelden sowieso al strengere voorwaarden en procedures.

L'article 126 de la loi relative aux communications électroniques prévoit maintenant des délais de conservations différentiés. Ce cadre est encore renforcé par les modifications à l'article 88bis, qui prévoient une différenciation en ce qui concerne les délais pour la demande de données.

Artikel 126 van de wet betreffende de elektronische communicatie voorziet nu verschillende bewaartermijnen. Dit kader wordt nog versterkt door de wijzigingen in artikel 88bis, die voorzien in een differentiatie in termijnen voor wat betreft het opvragen van gegevens.

Les modifications que le présent avant-projet de loi apporte à l'article 88bis sont de trois ordres :

- limitation du champ d'application et des délais dans lesquels les données peuvent être demandées ;
- protection du secret professionnel des avocats et des médecins ;
- adaptations terminologiques et adaptations à l'évolution constante de la technologie.

Au total, huit modifications sont apportées à l'article. Elles sont commentées point par point ci-après.

1°

La première modification concerne le champ d'application dans lequel les données peuvent être demandées et donc également le principe de proportionnalité. Dans l'état actuel du droit, les données de trafic et de localisation peuvent être demandées lors de la recherche de toutes les infractions possibles. Dans la mesure où le juge d'instruction est la personne habilitée à ordonner la mesure et où une instruction judiciaire est dès lors en cours, il est pratiquement exclu d'ordonner cette mesure pour des infractions minimes. Le gouvernement estime néanmoins nécessaire d'introduire une limite claire dans l'article. Désormais, la mesure ne pourra être utilisée que s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

La collecte de telles données constitue une limitation des droits et libertés individuels et, en vertu du principe de proportionnalité, ne peut par conséquent être autorisée qu'en cas d'infraction proportionnelle à l'ordre juridique. Le même seuil est utilisé pour la délivrance d'un mandat d'arrêt (article 16 de la loi du 20 juillet 1990 relative à la détention préventive) et des mesures d'instruction analogues telles l'interception du courrier (article 46ter) ainsi que la collecte de renseignements sur les comptes bancaires (article 46quater).

Par la même occasion, la terminologie est adaptée dans cet alinéa 1er du § 1er. Dans l'article 46bis, il est en effet question du « concours de l'opérateur

De wijzigingen die huidig voorontwerp van wet in artikel 88bis aanbrengt, zijn van drieërlei aard:

- Beperking van het toepassingsgebied én de termijnen waarvoor de gegevens opgevraagd kunnen worden;
- Bescherming van het beroepsgeheim van advocaten en artsen;
- Terminologische aanpassingen en aanpassingen aan de voortschrijdende technologische evolutie.

In totaal worden er acht wijzigingen aangebracht in het artikel. Deze worden hierna punt per punt toegelicht.

1°

De eerste wijziging betreft het toepassingsgebied waarvoor de gegevens kunnen opgevraagd worden, en dus ook de proportionaliteitsvereiste. In de huidige stand van het recht kunnen verkeers- en lokalisatiegegevens opgevraagd worden bij de opsporing naar alle mogelijke misdrijven. Aangezien het de onderzoeksrechter is die de maatregel kan bevelen, en er dus een gerechtelijk onderzoek loopt, is het zo goed als uitgesloten dat men deze maatregel zal bevelen voor minieme misdrijven. Niettemin acht de Regering het noodzakelijk om een duidelijke grens in te voeren in het artikel. Voortaan zal de maatregel enkel kunnen gebruikt worden wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben.

Het inwinnen van dergelijke gegevens vormt een beperking van de individuele rechten en vrijheden en kan derhalve, ingevolge het proportionaliteitsbeginsel, slechts worden toegestaan, ingeval van een evenredige inbreuk op de rechtsorde. Dezelfde drempel wordt gehanteerd voor het verlenen van een aanhoudingsmandaat (artikel 16 van de wet van 20 juli1990 betreffende de voorlopige hechtenis), en gelijkaardige onderzoeksmaatregelen zoals het onderscheppen van post (artikel 46ter), en het inwinnen van inlichtingen betreffende bankrekeningen (artikel 46quater).

Tegelijk wordt in dit eerste lid van § 1 de terminologie aangepast. Artikel 46bis spreekt immers over "de medewerking van de operator

d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique » tandis que l'article 88bis utilise encore l'ancienne terminologie : « l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication ». Il est proposé d'uniformiser la terminologie. Ce sera également le cas plus loin dans l'article.

Enfin, les données pouvant faire l'objet d'un repérage sont définies aux points 1° et 2° de l'alinéa 1er du § 1er. Il y est également encore question de « télécommunication », terme à présent remplacé par « communication électronique ». En outre, les termes « données d'appel » et « appels » ne sont plus adaptés aux possibilités technologiques actuelles. Il est proposé d'utiliser le terme « données de trafic » par analogie avec la loi du 13 juin 2005 relative aux communications électroniques et de remplacer le mot « appels » par « communications électroniques ».

2°

La modification apportée au § 1er, alinéa 2, est purement terminologique. Il peut être renvoyé aux explications données au point 1°.

3°

Dans l'état actuel du droit, le juge d'instruction doit indiquer les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée. Il paraît indiqué au gouvernement d'étendre cette motivation par analogie avec l'article 46bis (qui constitue en soi une infraction moindre à la vie privée que l'article 88bis) : pour cette mesure, la motivation doit refléter la proportionnalité en tenant compte de la vie privée et de la subsidiarité à tout autre devoir d'enquête. L'alinéa 3 du § 1er est donc modifié en ce sens.

4°

L'alinéa 4 du § 1er dispose que le juge d'instruction doit préciser la durée de la mesure, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement.

van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst", terwijl in artikel 88bis nog de oude terminologie "de operator van een telecommunicatienetwerk of van de verstrekker van een telecommunicatiedienst". Er wordt voorgesteld de terminologie uniform te maken. Dit gebeurt ook verder in het artikel.

Tot slot, in de punten 1° en 2° van het eerste lid van § 1 wordt bepaald welke gegevens opgespoord kunnen worden. Ook hier spreekt men nog over "telecommunicatie", dat nu vervangen wordt door "elektronische communicatie". Daarenboven zijn de termen "oproepgegevens" en "oproepen" niet meer aangepast aan de huidige technologische mogelijkheden. Voorgesteld wordt om te spreken over "verkeersgegevens", naar analogie met de wet van 13 juni 2005 betreffende de elektronische communicatie, en het woord "oproepen" te vervangen door "elektronische communicaties".

2°

De wijziging in § 1, tweede lid is louter terminologisch. Er kan verwezen worden naar wat toegelicht werd onder punt 1°.

3°

In de huidige stand van het recht dient de onderzoeksrechter de feitelijke omstandigheden van de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift te vermelden. Het lijkt de Regering aangewezen om deze motivering uit te breiden naar analogie met artikel 46bis (op zich een mindere inbreuk op de privacy dan artikel 88bis): voor deze maatregel dient de motivering de proportionaliteit te weerspiegelen met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. Het derde lid van §1 wordt dus in deze zin gewijzigd.

4°

Het vierde lid van § 1 bepaalt dat de onderzoeksrechter de duur van de maatregel dient te vermelden, die niet langer mag zijn dan twee maanden vanaf het bevelschrift, onverminderd een hernieuwing.

Cette disposition s'applique toutefois uniquement à la collecte de données en temps réel puisqu'il est question d'une durée *à dater* de l'ordonnance. Cela signifie que le juge d'instruction ne peut placer sous surveillance et collecter les données de trafic et de localisation des communications électroniques du suspect que durant une période deux mois. Sur cette base, la Cour de cassation a estimé qu'une ordonnance motivée au sens de l'article 88bis n'est pas requise lorsque la mesure porte sur une période écoulée au moment où la mesure est ordonnée (Cass., 16 avril 2003, D.D.P. 2003n 1183). Il n'est donc pas déterminé légalement jusqu'où le juge d'instruction peut remonter dans le temps dans le cadre de la demande de ces données et la demande de repérage du juge d'instruction peut donc porter sur une durée plus longue que deux mois.

Deze bepaling geldt echter alleen voor de collectie van gegevens in real time, vermits er sprake is van een periode *vanaf* het bevelschrift. Het betekent dat de onderzoeksrechter de verkeers- en lokalisatiegegevens van de elektronische communicatie van een verdachte slechts voor een periode van twee maanden onder toezicht kan plaatsen en verzamelen. Op basis hiervan heeft het Hof van Cassatie geoordeeld dat een gemotiveerde beschikking in de zin van artikel 88bis niet vereist is wanneer de maatregel betrekking heeft op een periode die verlopen is op het ogenblik dat de maatregel bevolen wordt (Cass 16 april 2003, R.D.P. 2003n 1183). Er wordt dus niet wettelijk bepaald hoelang de onderzoeksrechter kan teruggaan in het verleden bij de opvraging van deze gegevens, en dus kan de zoekopdracht van de onderzoeksrechter slaan op een periode van langer dan twee maanden.

Dans le nouveau § 2 de l'article 88bis, une nouvelle différenciation est à présent établie : pour certaines données, le juge d'instruction ne pourra remonter dans le temps que pour une durée limitée. Il est dès lors indiqué que le juge d'instruction indique dans son ordonnance jusqu'où il souhaite remonter dans le temps dans le repérage de données, conformément à ce nouveau § 2. Bien entendu, cela ne signifie pas que le juge d'instruction ne peut pas imposer dans son ordonnance un délai plus court que celui prévu au § 2.

In de nieuwe § 2 van artikel 88bis wordt nu een differentiatie ingevoerd: voor bepaalde gegevens zal de onderzoeksrechter slechts voor een beperkte periode kunnen teruggaan in het verleden Het is dan ook aangewezen dat de onderzoeksrechter in zijn bevelschrift dient aan te geven hoe ver in het verleden hij wenst terug te gaan bij het opsporen van gegevens, overeenkomstig deze nieuwe § 2. Dit betekent uiteraard niet dat de onderzoeksrechter geen kortere termijn kan opleggen in het bevelschrift dan deze voorzien in § 2.

5°

5°

L'article 88bis est, avec l'article 90ter concernant l'interception de télécommunications, une des rares mesures d'instruction que le juge d'instruction ne peut ordonner verbalement en cas d'urgence. Pourtant, on peut s'imaginer que dans certains cas, ces mesures doivent pouvoir être mises en œuvre rapidement, par exemple à la suite d'une prise d'otages ou d'un enlèvement, auxquels cas il convient de pouvoir localiser un téléphone mobile aussi rapidement que possible ou de mettre rapidement sur écoute la communication entre auteurs et complices. Ou encore lorsqu'une telle mesure doit être ordonnée au milieu de la nuit ou en dehors des heures de bureau. Cela doit pouvoir se faire rapidement et efficacement.

Artikel 88bis is, samen met artikel 90ter betreffende de interceptie van communicatie, één van de weinige onderzoeksmaatregelen waarin het bevel van de onderzoeksrechter in spoedeisende gevallen niet mondeling kan worden gegeven. Nochtans kan men zich voorstellen dat in bepaalde gevallen deze maatregelen snel ten uitvoer gelegd moeten kunnen worden, bijvoorbeeld naar aanleiding van een gijzeling of een ontvoering waarbij zo snel mogelijk een mobiele telefoon gelokaliseerd dient te worden, of waarbij de communicatie tussen daders en mededaders snel afgeluisterd moet kunnen worden. Of nog wanneer een dergelijke maatregel dient bevolen te worden in het midden van de nacht of buiten de kantooruren. Dit moet snel en efficiënt kunnen gebeuren.

En outre, les juges d'instruction sont eux-mêmes demandeurs de la possibilité d'ordonner verbalement dans ces cas, avec confirmation écrite ultérieure dans les meilleurs délais. Une comparaison peut être établie avec un certain nombre d'autres mesures d'instruction comme l'intervention différée (article 40bis), le contrôle visuel discret (articles 46quinquies et 89ter), l'observation (article 47sexies) et l'infiltration (article 47octies). C'est la raison pour laquelle le présent article de l'avant-projet de loi permet, pour l'article 88bis aussi, que la mesure de repérage ou de localisation de télécommunications puisse être ordonnée verbalement. Dans ce cas, la mesure doit être confirmée dans les meilleurs délais par une ordonnance motivée dans la forme requise à l'article 88bis, § 1er, alinéas 3 et 4.

Bovendien zijn de onderzoeksrechters zelf vragende partij om in deze gevallen een mondeling bevel te kunnen geven, waarna dit bevel zo snel mogelijk schriftelijk bevestigd wordt. Men kan dit vergelijken met een aantal andere onderzoeksmaatregelen zoals de uitgestelde tussenkomst (art. 40bis), de inkijkoperatie (art. 46quinquies en 89ter), de observatie (art. 47sexies), en de infiltratie (art. 47octies). Vandaar dat huidig artikel van het voorontwerp van wet het ook in het geval van artikel 88bis mogelijk maakt dat de maatregel tot opsporing of lokalisatie van communicatie mondeling kan worden bevolen. Het bevel moet dan zo spoedig mogelijk worden bevestigd bij een met redenen omkleed bevelschrift zoals vereist wordt door artikel 88bis, § 1, derde en vierde lid.

6°

6°

La Cour de Justice a considéré que la directive ne contenait pas de critère objectif limitant les personnes autorisées à accéder aux données et à les utiliser ultérieurement au nombre strictement nécessaire dans la perspective des objectifs à atteindre.

Het Hof van Justitie overwoog dat de richtlijn geen objectief criterium bevatte ter beperking van het aantal personen dat werd geautoriseerd voor de toegang en het verdere gebruik van de gegevens, tot hetgeen strikt noodzakelijk was in het licht van de te bereiken doelen.

Au § 1er, un principe de proportionnalité a déjà été inséré en limitant le champ d'application de l'article 88bis aux infractions pour lesquelles il existe des indices sérieux que ces infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde.
Il est à présent également répondu à la préoccupation de la Cour de Justice en limitant davantage l'accès aux données sur la base de la gravité de l'infraction en question. Outre le délai qui s'applique à la conservation des données par les opérateurs et les fournisseurs de services, le délai d'accès réel du juge d'instruction aux données est un élément supplémentaire pour déterminer la nécessité et la proportionnalité de cette mesure.

In § 1 werd al een proportionaliteitsvereiste ingevoegd door het toepassingsgebied van artikel 88bis te beperken tot misdrijven waarvoor er ernstige aanwijzingen zijn dat zij een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben. Aan de bezorgdheid van het Hof van Justitie wordt nu ook vorm gegeven doordat de toegang tot de gegevens verder wordt beperkt aan de hand van de ernst van het betreffende misdrijf. Naast de termijn die geldt voor het bewaren van gegevens door de operatoren en dienstenverstrekkers, is de termijn voor de daadwerkelijke toegang tot de gegevens door de onderzoeksrechter een extra element voor het vaststellen van de noodzakelijkheid en de proportionaliteit van deze maatregel.

Les données dont il est question au § 1er de l'article 88bis doivent en principe être conservées par les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communication électronique sur la base de l'article 126 de la loi relative aux communications électroniques. Il s'agit des données visées aux alinéas 3 et 4 de l'article 126, § 3, pour lesquelles le délai de conservation est fixé à [9/12] mois à partir

De gegevens waarvan sprake in § 1 van artikel 88bis moeten in principe bewaard worden door de operatoren van elektronische communicatienetwerken en dienstenverstrekkers van elektronische communicatiediensten op basis van artikel 126 van de wet betreffende de elektronische communicatie. Het gaat om de gegevens bedoeld in het derde en vierde lid van artikel 126, § 3, waarvoor de bewaartermijn op

de la date de la communication.

À la différence de ce qui était en vigueur précédemment, le juge d'instruction ne peut toutefois recourir à la totalité du délai de conservation de op [9/12] mois que lorsqu'il est question d'infractions visées à l'article 90ter, §§ 2 et 4, ou qui sont commises dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou qui sont de nature à entraîner un emprisonnement de cinq ans ou une peine plus lourde (premier tiret du § 2). Pour des infractions de moindre gravité, les données peuvent uniquement être requises pour une période de six mois préalable à l'ordonnance (deuxième tiret du § 2). Dans cette dernière situation, les données sont donc encore en possession des opérateurs ou des fournisseurs de services, mais le juge d'instruction ne peut plus les requérir. Cela signifie en fait que la durée de disponibilité des données conservées pour la recherche de ces infractions est ramenée de op [9/12] à six mois. Ainsi, sur la base d'un critère objectif, en l'occurrence la gravité de l'infraction en question, une différenciation plus précise est établie dans la mise à disposition des données à l'intention du juge d'instruction. Il est une nouvelle fois rappelé que pour des infractions pouvant qui sont de nature à entraîner une peine d'emprisonnement de moins d'un an, les données conservées ne peuvent en aucun cas être demandées.

Il est explicitement renvoyé aux données visées à l'article 126 de la loi relative aux communications électroniques, données qui doivent obligatoirement être conservées par les opérateurs et les fournisseurs de services aux fins de l'instruction d'infractions et de l'application des articles 46bis et 88bis. Outre ces données à conserver obligatoirement, les opérateurs et les fournisseurs de services peuvent toutefois également conserver d'autres données encore sur la base d'autres dispositions légales, notamment pour les besoins de la facturation et du marketing. Dans la mesure où ces données sont disponibles, elles doivent également être mises à la disposition du juge d'instruction, même si ce ne sera possible que pour les infractions les plus graves, à savoir celles visées à l'article 90ter, §§ 2 à 4, ou qui sont commises dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou

[9/12] maanden is bepaald vanaf de datum van de communicatie.

De bewaartermijn van op [9/12] maanden kan, anders dan tot nu toe, door de onderzoeksrechter echter alleen volledig worden benut wanneer sprake is van strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek, of een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben (eerste streepje van § 2). Bij lichtere misdrijven mogen de gegevens slechts voor een periode van zes maanden voorafgaand aan het bevelschrift worden gevorderd (tweede streepje van § 2). In die laatste situatie zijn de gegevens binnen de bewaartermijn dus nog wel in bezit van de operatoren of dienstenverstrekkers, maar kan de onderzoeksrechter de gegevens niet meer vorderen. Dit betekent in feite dat de periode van beschikbaarheid van de bewaarde gegevens voor de opsporing van deze misdrijven wordt teruggebracht van op [9/12] naar zes maanden. Zo wordt op basis van een objectief criterium, met name de ernst van het betreffende strafbare feit, nadere differentiatie aangebracht in de beschikbaarstelling van de gegevens aan de onderzoeksrechter. Er wordt ook nogmaals herinnerd dat voor strafbare feiten die een gevangenisstraf van minder dan een jaar tot gevolg kunnen hebben, de bewaarde gegevens helemaal niet opgevraagd kunnen worden.

Er wordt expliciet verwezen naar de gegevens bedoeld in artikel 126 van de wet betreffende de elektronische communicatie, gegevens die verplicht bewaard moeten worden door de operatoren en dienstenverstrekkers ten behoeve van het onderzoek naar strafbare feiten en de toepassing van de artikelen 46bis en 88bis. Naast deze verplicht te bewaren gegevens kunnen operatoren en dienstenverstrekkers echter ook nog andere gegevens bewaren, op basis van andere wettelijke bepalingen, onder meer met het oog op facturatie en marketing. In de mate dat die gegevens beschikbaar zijn, dienen zij ook ter beschikking gesteld worden van de onderzoeksrechter, zij het dat dit enkel mogelijk zal zijn voor de zwaarste misdrijven, nl. de misdrijven zoals bedoeld in artikel 90ter, §§ 2 tot 4, of gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het

qui sont de nature à entraîner une peine d'emprisonnement de cinq ans ou une peine plus lourde. Dans ce cadre, le juge d'instruction peut remonter plus loin dans le temps que les op [9/12] mois visés à l'alinéa 1er et doit l'indiquer expressément dans son ordonnance. Cette disposition figure à l'alinéa 2 du deuxième tiret de ce nouveau § 2. Cette possibilité n'est toutefois pas prévue pour les infractions de moindre gravité : pour ces infractions, le juge d'instruction ne peut donc requérir aucune donnée supplémentaire conservée sur la base de dispositions légales autres que l'article 126 de la loi relative aux communications électroniques.

Strafwetboek, of een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben. De onderzoeksrechter kan daarbij verder in het verleden teruggaan dan de op [9/12] maanden bedoeld in het eerste lid, en dient dit uitdrukkelijk te bepalen in zijn bevelschrift. Dit wordt bepaald in het tweede lid van het eerste streepje van de nieuwe § 2. Deze mogelijkheid is echter niet voorzien voor de lichtere misdrijven: daarvoor kan de onderzoeksrechter dus geen bijkomende gegevens die bewaard worden op basis van andere wettelijke bepalingen dan artikel 126 WEC opvorderen.

7°

7°

Au point B.10.1 de son arrêt, la Cour constitutionnelle a précisé que la législation en matière de conservation des données s'applique sans aucune exception à des personnes dont les communications sont soumises au secret professionnel. Indépendamment du fait que la législation sur la conservation des données ne porte pas sur le contenu de la communication, il semble en effet indiqué d'insérer une certaine protection à l'égard des avocats et des médecins, des catégories professionnelles qui sont par excellence exposées au risque d'être confrontées à des suspects avec qui, en raison de leur situation professionnelle, ils entretiennent une relation de confiance.

Het Grondwettelijk Hof heeft in punt B.10.1 van haar arrest gezegd dat de wetgeving omtrent dataretentie zonder enige uitzondering van toepassing was op personen wiens communicatie onder het beroepsgeheim valt. Los van het feit dat de dataretentiewetgeving geen betrekking heeft op de inhoud van de communicatie, lijkt het inderdaad aangewezen om een zekere bescherming in te voeren voor advocaten en artsen, de beroepscategorieën die bij uitstek het gevaar lopen om geconfronteerd te worden met verdachten waarmee zij door hun beroepssituatie in een vertrouwelijke relatie verkeren.

Le nouveau § 3 limite la possibilité d'appliquer la mesure aux avocats et aux médecins de la manière déjà en vigueur actuellement dans le cas notamment de l'observation effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile (article 56bis) ou de l'écoute téléphonique (article 90octies). À l'instar de ce qui a été prévu pour ces mesures, l'article 88bis ne pourra être appliqué que si l'avocat ou le médecin est lui-même soupçonné d'avoir commis l'infraction ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées au § 1er utilisent ses moyens de communication électronique. L'intervention des organisations professionnelles respectives est également prévue.

De nieuwe § 3 beperkt de mogelijkheid om de maatregel toe te passen op advocaten en artsen op dezelfde manier als nu al het geval is bij bijvoorbeeld de observatie met technische hulpmiddelen met zicht in een woning (artikel 56bis), of de telefoontap (artikel 90octies). Zoals ook bij die maatregelen is voorzien, zal artikel 88bis enkel toegepast kunnen worden indien de advocaat of de arts zelf van het misdrijf of deelname daaraan wordt verdacht of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in § 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen. Ook de tussenkomst van de respectievelijke beroepsorganisaties wordt voorzien.

8°

8°

Enfin, dans l'ancien § 2 (qui deviendra le § 4) qui

Tot slot wordt in de oude § 2, die nu § 4 zal worden

impose le concours des opérateurs et des fournisseurs de services, la terminologie sera également adaptée comme détaillé au point 1°.

en waarin de medewerking van operatoren en dienstenverstrekkers wordt opgelegd, de terminologie aangepast zoals al omschreven onder punt 1°.

Art. 10

Dit artikel vervolledigt artikel 90*decies* van het Wetboek van Strafvordering. Het jaarlijkse verslag van de minister van Justitie dat door dit artikel wordt voorgeschreven, zal voortaan ook statistische informatie bevatten over de bewaring van gegevens zoals bedoeld door artikel 126 van de wet betreffende de elektronische communicatie.

Art. 10

Cet article complète l'article 90*decies* du Code d'instruction criminelle. Le rapport annuel par le ministre de la Justice prévu par cet article contiendra désormais des informations statistiques concernant la conservation des données visée à l'article 126 de la loi relative aux communications électroniques.

Hoofdstuk IV. Bepalingen tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Chapitre IV. Dispositions modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 11 (wijziging art. 13 W.I&V)

1° In het eerste lid van artikel 13 bestaat de voorgestelde wijziging uit een materiele correctie van een fout in de vertaling. In de Franse tekst spreekt men van "de rechercher des informations" en niet van "des renseignements".

Art. 11 (modification art. 13 loi Renseignement)

1° A l'alinéa 1er de l'article 13, la modification proposée consiste en une correction matérielle qui résulte d'une erreur de traduction. Dans la version française du texte, on parle en effet " de rechercher des informations" et non "des renseignements".

2° Het derde lid van artikel 13 heeft tot doel de bescherming van de informatiebronnen van de inlichtingen- en veiligheidsdiensten, met inbegrip van persoonsgegevens die, bijvoorbeeld, geleverd werden door menselijke bronnen of buitenlandse inlichtingendiensten maar die ook kunnen voortkomen uit technische bronnen.

2° L'alinéa 3 de l'article 13 vise à protéger toutes les sources d'informations des services de renseignement et de sécurité, en ce compris les données à caractère personnel, qu'elles aient été fournies par des sources humaines ou des services de renseignement étrangers, par exemple, mais aussi qu'elles proviennent de sources techniques.

Persoonsgegevens die verzameld werden met inzet van de specifieke methode voor het verzamelen van gegevens van art. 18/8 en waarbij beroep gedaan wordt op een operator of een dienstenverstrekker voor het opsporen van verkeersgegevens en voor de lokalisatie van de oorsprong of de bestemming van de elektronische communicatie, vallen onder deze bescherming die onontbeerlijk is ten aanzien van de persoonlijke levenssfeer.

Les données à caractère personnel recueillies par la mise en œuvre de la méthode spécifique de recueil de données de l'art. 18/8 impliquant le recours à un opérateur ou un fournisseur de services en vue du repérage des données de trafic et de la localisation de l'origine ou de la destination de communications électroniques, feront l'objet de cette protection indispensable au respect de la vie privée.

3° Om de bescherming van deze informatie, inlichtingen en persoonsgegevens te vervolledigen, wijst het nieuwe vierde lid van artikel 13 nogmaals op een fundamenteel principe in de organieke wet met betrekking tot de toegang tot de verzamelde gegevens met het oog op hun verwerking met respect van het finaliteitsprincipe: de nood tot kennisname.

3° Pour compléter la protection de ces informations, renseignements et données à caractère personnel, le nouvel alinéa 4 de l'article 13 rappelle dans la loi organique un principe fondamental lié à l'accès aux données recueillies en vue de leur traitement dans le respect du principe de finalité : le besoin d'en connaître.

Het is ook zo dat agenten van de inlichtingen- en veiligheidsdiensten slechts toegang kunnen hebben tot informatie, inlichtingen en persoonsgegevens, met inbegrip van deze die voortkomen uit elektronische communicatie, voor zover deze nuttig zijn voor de uitoefening van hun taken en opdracht.

Dit is bovendien een fundamenteel principe voor de werking van een inlichtingen- en veiligheidsdienst.

Art. 12 (wijziging art. 18/3 W.I&V)

1° Het nieuwe artikel 18/3, §2 bepaalt de vermeldingen die verplicht moeten worden opgenomen in de beslissing van het diensthoofd.

Naast de klassieke vermeldingen opgesomd in artikel 18/3, §3 die betrekking hebben op de maandelijkse lijsten die aan de Commissie dienen te worden overgemaakt, namelijk,

- de aard van de specifieke methode,
- de graad van ernst van de dreiging die het rechtvaardigt,
- de natuurlijke perso(o)n(en) of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp van de methode uitmaken,
- het te gebruiken technisch hulpmiddel,
- de periode waarin de methode kan worden aangewend,

voorziet de nieuwe tekst in bijkomende garanties voor het aanwenden van specifieke methodes door nieuwe vermeldingen op te leggen die in de beslissing van het diensthoofd moeten staan, namelijk:

- de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit en het verband tussen het doel van de methode en de potentiele dreiging,
- voor wat meer bepaald de toepassing van artikel 18/8 betreft, dat betrekking heeft op de opsporing van verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarheen de oproepen worden gezonden of werden gezonden en van de lokalisatie van de oorsprong of de bestemming van de elektrische communicatie, de

C'est ainsi que les agents des services de renseignement et de sécurité ne pourront avoir accès à ces informations, renseignements et données à caractère personnel, en ce compris celles qui résultent des communications électroniques, que pour autant que ceux-ci soient utiles dans l'exercice tant de leur fonction que de leur mission.

Il s'agit en outre d'un principe fondamental de fonctionnement d'un service de renseignement et de sécurité.

Art. 12 (modification art. 18/3 loi Renseignement)

1° L'article 18/3, §2 nouveau énonce les mentions qui doivent obligatoirement figurer dans la décision du dirigeant du service.

Outre les mentions classiques qui étaient énumérées à l'article 18/3, §3 relatif aux listes mensuelles à communiquer à la Commission, à savoir,

- la nature de la méthode spécifique,
- le degré de gravité de la menace qui la justifie,
- la/les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode,
- le moyen technique utilisé,
- la période pendant laquelle la méthode peut être mise en œuvre,

le nouveau texte apporte des garanties supplémentaires pour la mise en œuvre des méthodes spécifiques, en rendant obligatoires de nouvelles mentions dans la décision du dirigeant du service notamment :

- les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité et le lien entre la cible de la méthode et la menace potentielle,
- et en ce qui concerne plus particulièrement l'application de l'article 18/8 relatif au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés et à la localisation de l'origine ou de la destination de communications électroniques, la motivation de la durée de la période à laquelle a trait la collecte de données.

motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft.

3° §3 wordt vervangen door § 2, eerste lid betreffende de maandelijkse lijsten en wordt aangevuld met een tweede lid, luidende als volgt: "Deze lijsten bevatten de gegevens bedoeld in § 2, 1° à 3°, 5° en 7°.".

3° Le §3 est remplacé par l'alinéa 1er du § 2 relatif aux listes mensuelles et est complété par un deuxième alinéa rédigé comme suit : « Ces listes comprennent les données visées au § 2, 1° à 3°, 5° et 7°. ».

4° Het derde lid van §1 met betrekking tot het aanwenden van specifieke methodes ten opzichte van advocaten, artsen en journalisten, voorziet in een bijzondere beschermingsprocedure voor deze categorieën van personen, wordt §5 van artikel 18/3.

4° L'alinéa 3 du §1er relatif à la mise en œuvre des méthodes spécifiques à l'égard des avocats, médecins et journalistes, lequel prévoit une procédure de protection particulière pour ces catégories de personnes, devient le §5 de l'article 18/3.

5° Het vierde lid van §1 dat betrekking heeft op het regelmatige informeren van het diensthoofd door een inlichtingenofficier die is aangesteld om de aanwending van de specifieke methode op te volgen, wordt §7 van artikel 18/3; de §6 heeft betrekking (zie supra) op de controle door de Commissie.

5° L'alinéa 4 du §1er qui concerne l'information régulière du dirigeant du service par l'officier de renseignement désigné pour le suivi de la mise en œuvre de la méthode devient le §7 de l'article 18/3, le §6 ayant trait (voir supra) au contrôle de la Commission.

6° De toevoeging van een nieuw §8 heeft tot doel om, in toepassing van het principe van de proportionaliteit, te specifiëren wat er dient te gebeuren bij de beëindiging van een methode indien een onwettigheid wordt vastgesteld, of wanneer de dreiging die die haar rechtvaardigt niet meer bestaat, of wanneer zij niet meer nuttig is.

6° L'insertion d'un nouveau § 8 a pour objectif de préciser, en application du principe de proportionnalité, qu'il doit être mis fin à une méthode dès qu'il est constaté une illégalité, ou que la menace qui l'a justifiée n'existe plus, ou qu'elle n'est plus utile.

Art. 13 (wijziging art. 18/8 W.I&V)

Art. 13 (modification art. 18/8 loi Renseignement)

Dit artikel bevat een aantal wijzigingen aan artikel 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Cet article comporte un certain nombre de modifications à l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Het Grondwettelijk Hof stelt in zijn reeds geciteerde arrest van 11 juni 2015 dat er bij wet geen enkele materiële of procedurele voorwaarde vastgelegd is met betrekking tot de toegang tot de bewaarde gegevens (overweging B.10.3). Opgemerkt moet worden dat het Hof hierbij voorbij gaat aan de procedurele voorwaarden voorzien in de artikelen 18/3, 18/7 en 18/8 van de wet van 30 november 1998. Het opvragen van identificatie, verkeers- en lokalisatiegegevens is namelijk een specifieke inlichtingenmethode die gemachtigd wordt door het diensthoofd en pas ten uitvoer kan gelegd worden na kennisgeving aan de BIM-Commissie (zie MvT bij artikel 18/3).

Dans son arrêt du 11 juin 2015 déjà cité, la Cour constitutionnelle a souligné que la loi ne fixe aucune condition matérielle ou procédurale concernant l'accès aux données conservées (considérant B.10.3). Il convient de préciser à cet égard que la Cour ne fait pas référence aux conditions de procédure prévues aux articles 18/3, 18/7 et 18/8 de la loi du 30 novembre 1998. La demande de données d'identification, de trafic et de localisation constitue en effet une méthode spécifique de recueil des données soumise à l'autorisation du chef de service et qui ne peut être mise en oeuvre qu'après en avoir informé la Commission MRD (voir EdM à l'article 18/3).

Om tegemoet te komen aan de bezorgdheden van het Hof, kiest de Regering er voor om extra waarborgen in te schrijven in artikel 18/8, dat betrekking heeft op het opvragen van verkeers- en lokalisatiegegevens. Deze gegevens zijn immers meer privacygevoelig dan de identificatiegegevens bedoeld in artikel 18/7.

Het Hof heeft er ook op gewezen dat, wat de bewaarperiode van de gegevens betreft, er geen enkel onderscheid gemaakt wordt tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken persoon (overweging B.10.4.).

Artikel 126 van de wet betreffende de elektronische communicatie voorziet nu verschillende bewaartermijnen. Dit kader wordt nog versterkt door de wijzigingen in artikel 18/8, die voorzien in een differentiatie in termijnen waarbinnen verkeers- en lokalisatiegegevens kunnen worden opgevraagd.

Het huidig voorontwerp van wet wijzigt artikel 18/8 op twee punten:

- Beperking van het toepassingsgebied én de termijnen waarvoor de gegevens opgevraagd kunnen worden;
- Terminologische aanpassingen en aanpassingen aan de voortschrijdende technologische evolutie.

1°

De woorden “bij schriftelijke beslissing” worden geschrapt gezien zij een herhaling vormen van de procedure in artikel 18/3 die stelt dat een specifieke methode slechts kan worden aangewend na een schriftelijke beslissing van het diensthoofd.

Ook moet worden opgemerkt dat de termen “oproepgegevens” en “oproepen” niet meer aangepast zijn aan de huidige technologische mogelijkheden. Voorgesteld wordt om te spreken over “verkeersgegevens”, naar analogie met de wet van 13 juni 2005 betreffende de elektronische communicatie, en het woord “oproepen” te vervangen door “elektronische communicaties”.

Afin de répondre aux préoccupations de la Cour, le Gouvernement a décidé d'inclure des conditions supplémentaires à l'article 18/8 en ce qui concerne la demande de données de localisation et de trafic. Ces données présentent en effet un caractère plus sensible au niveau de la vie privée que les données d'identification visées à l'article 18/7.

Par ailleurs, la Cour a également indiqué qu'en ce qui concerne la période de conservation des données, aucune distinction n’est opérée entre les catégories de données sur la base de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées (considérant B.10.4)

L'article 126 de la loi relative aux communications électroniques prévoit maintenant des délais de conservation différenciés. Ce cadre est encore renforcé par les modifications à l'article 18/8 qui prévoient d’opérer une différenciation entre les délais à respecter pour la demande de données de localisation et de trafic.

Les modifications apportées à l’article 18/8 par le présent avant-projet de loi sont de deux ordres:

- limitation du champ d’application et des délais dans lesquels les données peuvent être demandées,
- adaptations terminologiques et adaptations à l'évolution constante de la technologie.

1°

Les mots “par une décision écrite” sont supprimés. Ils constituent en effet une répétition de la procédure mentionnée à l’article 18/3 qui stipule qu’une méthode spécifique ne peut être mise en oeuvre qu’après avoir obtenu l’autorisation écrite du dirigeant du service.

Il convient également de préciser que les termes “données d’appel” et “appels” ne sont plus adaptés aux possibilités technologiques actuelles. Il est donc proposé d’utiliser le terme de “données de trafic” par analogie avec la loi du 13 juin 2015 relative aux communications électroniques, et de remplacer le mot “appels” par “communications électroniques”.

2°

De wijziging in § 1, tweede lid, is louter terminologisch. Er kan verwezen worden naar de toelichting onder punt 1°.

3°

Om tegemoet te komen aan overweging B.10.4. van het Hof wordt in artikel 18/8 een differentiatie ingevoerd in termijnen waarbinnen de inlichtingendiensten verkeers- en lokalisatiegegevens kunnen opvragen: voor bepaalde gegevens zal het diensthoofd slechts voor een beperkte periode kunnen teruggaan in het verleden, ook al worden de gegevens voor een langere periode bijgehouden door de netwerkoperator of dienstenverstrekker op basis van artikel 126 van de wet op de elektronische communicatie.

De verkeers- en lokalisatiegegevens waarvan sprake in § 1, eerste lid van artikel 18/8 moeten in principe bewaard worden door de operatoren van elektronische communicatienetwerken en dienstenverstrekkers van elektronische communicatiediensten op basis van artikel 126 van de wet betreffende de elektronische communicatie. Het gaat om de gegevens bedoeld in het derde en vierde lid van artikel 126, § 3, waarvoor de bewaartermijn 12 maanden bedraagt vanaf de datum van de communicatie.

De bewaartermijn van 12 maanden kan, anders dan tot nu toe, door inlichtingendiensten echter alleen volledig worden benut wanneer sprake is van een potentiëledreiging tegen de inwendige of uitwendige veiligheid van de staat of het wetenschappelijk en economisch potentieel van het land, de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen, de vervulling van de opdrachten van de strijdkrachten, de veiligheid van de Belgische onderdanen in het buitenland, het behoud van de militaire veiligheid, het beschermen van het geheim of het wetenschappelijk of economisch potentieel of elk ander fundamenteel belang van het land, in het geval deze dreiging betrekking heeft op een activiteit die verband kan houden met terrorisme, extremisme, spionage of de proliferatie van massavernietigingswapens.

Wanneer de potentiële dreiging uitgaat van

2°

La modification apportée au § 1er , alinéa 2, est purement terminologique. Il peut être renvoyé aux explications reprises au point 1°.

3°

Afin de répondre au considérant B.10.4 de la Cour, une différenciation a été introduite dans l'article 18/8 concernant les délais dans lesquels les services de renseignement peuvent demander des données de localisation et de trafic : pour certaines données, le dirigeant du service pourra remonter dans le passé dans une certaine limite seulement et ceci bien que l'opérateur de réseau ou le fournisseur de services soit autorisé à conserver ces données pendant une plus longue période conformément à l'article 126 de la loi relative aux communications électroniques.

Les données de localisation et de trafic dont il est question au §1, alinéa 1er de l'article 18/8 doivent en principe être conservées par les opérateurs de réseau de communication électronique et les fournisseurs de services de communication électronique conformément à l'article 126 de la loi relative aux communications électroniques. Il s'agit des données visées aux alinéas 3 et 4 de l'article 126, §3, dont le délai de conservation est de 12 mois à partir de la date de la communication.

A la différence de ce qui existait précédemment, les services de renseignement ne peuvent toutefois recourir à la totalité du délai de conservation de 12 mois qu'en présence d'une menace potentielle contre la sûreté intérieure ou extérieure de l'Etat ou le potentiel économique et scientifique du pays, l'intégrité du territoire national, les plans de défense militaires, l'accomplissement des missions des Forces armées, la sécurité des citoyens belges à l'étranger, le maintien de la sécurité militaire, la protection du secret ou le potentiel scientifique ou économique ou tout autre intérêt fondamental du pays, que dans le cas où cette menace concerne une activité qui peut avoir un lien avec le terrorisme, l'extrémisme, l'espionnage ou la prolifération d'armes de destruction massive.

Lorsque la menace potentielle émane d'activités en

activiteiten gelieerd aan inmenging, criminele organisaties of schadelijke sektarische organisaties, mogen de gegevens slechts voor een periode van 6 maanden opgevraagd worden. In die laatste situatie zijn de gegevens binnen de bewaartermijn dus nog wel in bezit van de netwerkoperatoren of dienstenverstrekkers, maar kan het diensthoofd de gegevens niet meer vorderen. Dit betekent in feite dat de periode van beschikbaarheid van de bewaarde gegevens voor het onderzoek naar een aantal dreigingen wordt teruggebracht van 12 maanden naar 6 maanden. Zo wordt op basis van de aard van de potentiële dreiging, een nadere differentiatie aangebracht in de beschikbaarstelling van de gegevens aan de inlichtingendiensten.

Er wordt expliciet verwezen naar de gegevens bedoeld in artikel 126 van de wet betreffende de elektronische communicatie, gegevens die verplicht bewaard moeten worden door de operatoren en dienstenverstrekkers ten behoeve van het onderzoek door de inlichtingendiensten en de toepassing van de artikelen 18/7 en 18/8 van de wet van 30 november 1998. Naast deze verplicht te bewaren gegevens kunnen operatoren en dienstenverstrekkers echter ook nog andere gegevens bewaren, op basis van andere wettelijke bepalingen, onder meer met het oog op facturatie en marketing. In de mate dat die gegevens beschikbaar zijn, dienen zij ook ter beschikking gesteld te worden van de inlichtingendiensten, zij het dat dit enkel mogelijk zal zijn in het kader van een onderzoek naar een potentiële dreiging gelieerd aan terrorisme, extremisme, spionage of proliferatie. De vordering van het diensthoofd kan daarbij verder in het verleden teruggaan dan de 12 maanden bedoeld in het eerste lid, 1°, en dient dit uitdrukkelijk te bepalen. Dit wordt bepaald in de tweede zin van art. 18/8, § 2, 1°. Deze mogelijkheid is echter niet voorzien in geval van potentiële dreigingen vermeld in 2°: daarvoor kan het diensthoofd dus geen bijkomende gegevens opvorderen die bewaard worden op basis van andere wettelijke bepalingen dan artikel 126 WEC.

4°

De huidige § 2 met betrekking tot de hoogdringendheidsprocedure wordt vernummerd

rapport avec l'ingérence, les organisations criminelles ou les organisations sectaires nuisibles, les données ne peuvent être demandées que pour une période de 6 mois. Dans cette dernière situation, les données se trouvent bien en possession des opérateurs de réseau ou des fournisseurs de services mais le dirigeant du service n'est plus autorisé à les requérir au-delà de ce délai. En d'autres termes, la période durant laquelle les données conservées sont disponibles pour l'enquête relative à un certain nombre de menaces est réduite de 12 mois à 6 mois. Ainsi, une différenciation supplémentaire est opérée sur la base de la nature de la menace potentielle en ce qui concerne la mise à disposition des données pour les services de renseignement.

Il est explicitement fait référence aux données visées à l'article 126 de la loi relative aux communications électroniques, données qui doivent obligatoirement être conservées par les opérateurs et fournisseurs de services à des fins d'enquête par les services de renseignement et pour l'application des articles 18/7 et 18/8 de la loi du 30 novembre 1998. Outre cette obligation de conservation des données, les opérateurs et fournisseurs de services sont toutefois autorisés à conserver d'autres données, sur la base d'autres dispositions légales, à des fins, entre autres, de facturation et de marketing. Dans la mesure où ces données sont disponibles, elles doivent également être mises à la disposition des services de renseignement, pour autant que ce soit à des fins d'enquête concernant une menace potentielle en rapport avec le terrorisme, l'extrémisme, l'espionnage ou la prolifération. Dans ce cadre, le dirigeant du service peut requérir la transmission de données antérieures au délai de 12 mois visé à l'alinéa 1er, 1°, et doit le mentionner expressément. Ceci est spécifié à la deuxième phrase de l'article 18/8, § 2, 1°. Cette possibilité n'est cependant pas prévue pour les menaces potentielles mentionnées en 2° : dans ce cas, le dirigeant du service n'est pas autorisé à requérir des données supplémentaires conservées sur la base de dispositions légales autres que l'article 126 de la loi relative aux communications électroniques.

4°

L'actuel § 2 concernant la procédure d'extrême urgence est renuméroté en § 4.

tot § 4.

De minister van Justitie, Le ministre de la Justice,

K. GEENS

De minister van Digitale Agenda, Telecom en Post Le ministre de l'Agenda numérique, des Télécom et de la Poste

Alexander De Croo

De minister van Defensie Le ministre de la Défense

Steven VANDEPUT

KONINKRIJK BELGIË

FEDERALE OVERHEIDSDIENST ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE

FEDERALE OVERHEIDSDIENST JUSTITIE

Datum - **Voorontwerp van wet betreffende de bewaring van gegevens in de elektronische-communicatiesector**

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

Gelet op de wetten op de Raad van State, gecoördineerd op 12 januari 1973, artikel 3, §§ 1 en 2;

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;

Gelet op het advies xxx van [DATUM] van de Raad van State;

Gelet op de raadpleging vanaf [DATUM] tot en met [DATUM] van het Interministerieel Comité voor Telecommunicatie en Radio-omroep en Televisie;

Gelet op het akkoord van het Overlegcomité van [DATUM] ;

Op de voordracht van de Minister van Digitale Agenda, Telecommunicatie en Post, de Minister van Justitie en de Minister van Defensie;

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ :

De Minister van Digitale Agenda, Telecommunicatie en Post en de Minister van Justitie zijn ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze

ROYAUME DE BELGIQUE

SERVICE PUBLIC FÉDÉRAL ÉCONOMIE, PME, CLASSES MOYENNES ET ÉNERGIE

SERVICE PUBLIC FÉDÉRAL JUSTICE

Date - **Avant-projet de loi relative à la conservation des données dans le secteur des communications électroniques**

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

Vu les lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973, l'article 3, §§1er et 2 ;

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 ;

Vu l'avis xxx émis le [DATE] par le Conseil d'Etat ;

Vu la consultation du [DATE] au [DATE] du Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision ;

Vu l'accord du Comité de concertation du [DATE] ;

Sur la proposition du Ministre de l'Agenda numérique, des Télécommunications et de la Poste, du Ministre de la Justice et du Ministre de la Défense ;

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

Le Ministre de l'Agenda numérique, des Télécommunications et de la Poste et le Ministre de la Justice sont chargés de présenter et de déposer au Parlement le projet de loi dont la

naam aan het Parlement voor te leggen en in te dienen:

teneur suit :

HOOFDSTUK 1. – Algemene bepaling	**CHAPITRE 1er – Dispositions générales**
Artikel 1. Deze wet regelt een aangelegenheid zoals bepaald in artikel 74 van de Grondwet.	**Article 1er.** La présente loi règle une matière visée à l'article 74 de la Constitution.
HOOFDSTUK 2. - Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie	**CHAPITRE 2. – Modifications de la loi du 13 juin 2005 relative aux communications électroniques**
Art. 2. In artikel 2 van de wet 13 juni 2005 betreffende de elektronische communicatie, gewijzigd bij de wetten van 18 mei 2009, 10 juli 2012 en 27 maart 2014, worden de volgende wijzigingen aangebracht:	Art. 2. Dans l'article 2 de la loi 13 juin 2005 relative aux communications électroniques, modifié par les lois des 18 mai 2009, 10 juillet 2012 et 27 mars 2014, les modifications suivantes sont apportées :
1° de bepaling onder 11° wordt vervangen als volgt:	1° le 11° est remplacé par ce qui suit :
" 11° "operator" : een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9; ";	« 11° "opérateur" : toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9; » ;
2° het artikel wordt aangevuld met een bepaling onder 74° luidende als volgt:	2° l'article est complété par un 74° rédigé comme suit :
" 74° "Oproeppoging zonder resultaat" : een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord. ".	« 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. ».
Art. 3. Artikel 125, § 2, gewijzigd bij de wetten van 10 juli 2012 en 27 maart 2014, van dezelfde wet wordt opgeheven.	Art. 3. L'article 125, § 2, de la même loi, modifié par les lois des 10 juillet 2012 et 27 mars 2014, est abrogé.
Art. 4. Artikel 126 van dezelfde wet wordt vervangen als volgt:	Art. 4. L'article 126 de la même loi est remplacé par ce qui suit:
"Art. 126 § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dienen de aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegang, van e-mail via het internet, de aanbieders van de onderliggende openbare elektronische-	« Art. 126. § 1er. Sans préjudice 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, les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les fournisseurs des réseaux publics de communications électroniques sous-jacents ainsi que les

communicatienetwerken, alsook de operatoren die een van deze diensten of netwerken verstrekken de in paragraaf 3 beoogde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

opérateurs fournissant un de ces services ou réseaux, conservent les données visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

Le présent article ne porte pas sur le contenu des communications.

De verplichting om de in paragraaf 3 bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:

L'obligation de conserver les données visées au paragraphe 3 s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

1° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de aanbieders van openbaar toegankelijke diensten voor elektronische communicatie of van een openbaar netwerk voor elektronische communicatie, of

1° en ce qui concerne les données de la téléphonie, générées ou traitées par les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

§ 2. Enkel de volgende overheden mogen op eenvoudig verzoek van de in paragraaf 1, eerste lid, beoogde aanbieders en operatoren data ontvangen die worden bewaard krachtens dit artikel om de redenen en volgens de voorwaarden opgesomd hieronder:

§ 2. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

1° De gerechtelijke autoriteiten, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken, voor de uitvoering van de in de artikelen 46bis en 88bis van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen.

1° Les autorités judiciaires, en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46bis et 88bis du Code d'instruction criminelle et dans les conditions fixées par ces articles.

2° De inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te vervullen en volgens de

2° Les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans les conditions fixées par cette loi.

voorwaarden vastgelegd in deze wet.

3° Elke officier van gerechtelijke politie van het Instituut, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en dit artikel.

4° De hulpdiensten die hulp ter plaatse bieden, wanneer ze naar aanleiding van een noodoproep, van de betrokken aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen met behulp van de databank beoogd in artikel 107, § 2, derde lid, of onvolledige of onjuiste gegevens krijgen. Enkel de identificatiegegevens van de oproeper mogen worden gevraagd en uiterlijk binnen [24] uur na de oproep. De aanbieder of de operator voert een voorafgaande controle uit van de identiteit van de hulpdiensten.

5° De officier van gerechtelijke politie van de cel Vermiste Personen van de federale politie, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood, 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. Enkel de gegevens die zijn beoogd in paragraaf 3, de leden 1 tot 3, met betrekking tot de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan het verzoek om de gegevens te krijgen, mogen worden gevraagd aan de operator of de aanbieder in kwestie, hetzij rechtstreeks, hetzij via een door de Koning aangewezen politiedienst.

6° De Ombudsdienst voor telecommunicatie, met het oog op de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, conform de voorwaarden beoogd in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd. Het verzoek dient te worden

3° Tout officier de police judiciaire de l'Institut, en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et au présent article.

4° Les services d'urgence offrant de l'aide sur place, lorsque, à la suite d'un appel d'urgence, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'appelant à l'aide de la base de données visée à l'article 107, § 2, alinéa 3, ou obtiennent des données incomplètes ou incorrectes. Seules les données d'identification de l'appelant peuvent être demandées et au plus tard dans les [24] heures de l'appel. Le fournisseur ou l'opérateur effectue une vérification préalable de l'identité des services d'urgence.

5° L'officier de police judiciaire de la cellule disparition de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, 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. Seules les données visées au paragraphe 3, alinéas 1 à 3, relatives à la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données peuvent être demandées à l'opérateur ou au fournisseur concerné, soit directement, soit par l'intermédiaire d'un service de police désigné par le Roi.

6° Le Service de médiation pour les télécommunications, en vue de l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, conformément aux conditions visées à l'article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées. La demande est adressée au fournisseur ou à l'opérateur concerné dans les

gericht aan de betrokken aanbieder of operator binnen [8] dagen na het kwaadwillig gebruik van het netwerk of van de dienst.

[8] jours suivant l'utilisation malveillante du réseau ou du service.

Dit artikel doet geen afbreuk aan de mogelijkheid voor elke in het eerste lid vermelde autoriteit om, om dezelfde redenen en met inachtneming van de voorwaarden vermeld in het eerste lid, de gegevens te verkrijgen die zijn bewaard krachtens de artikelen 122 en 123.

Le présent article ne porte pas préjudice à la possibilité pour chaque autorité mentionnée dans l'alinéa 1er d'obtenir, pour les mêmes finalités et en respectant les conditions mentionnées dans l'alinéa 1er, les données conservées en application des articles 122 et 123.

De aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 3 onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld aan de autoriteiten beoogd in deze paragraaf kunnen worden meegedeeld en uitsluitend aan deze laatste.

Les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 3, soient accessibles de manière illimitée à partir de la Belgique et que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai aux autorités visées dans le présent paragraphe et uniquement à ces dernières.

Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden.

Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités.

§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin de leden 2, 3 en 4 specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

§ 3. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2, 3 et 4, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

De gegevens betreffende de communicatiediensten die worden verstrekt aan een abonnee of een gebruiker of die hij kan gebruiken via zijn eindapparatuur, met inbegrip van de volumes waarop hij heeft ingetekend en die werden verbruikt, worden gedurende twee maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

Les données relatives aux services de communications qui sont fournis à l'utilisateur ou à l'abonné ou qu'il peut utiliser à l'aide de son équipement terminal, y compris les volumes auxquels il a souscrit et qui ont été consommés, sont conservées pendant deux mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

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,

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 mais

inclusief het netwerkaansluitpunt, maar exclusief de gegevens waarin het vierde lid voorziet, worden bewaard gedurende op [9/12] maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, de tijdsregistratie, de identificatie van de eindapparatuur van waaruit of waaraan communicatie wordt of werd gericht, worden gedurende op [9/12] maanden bewaard vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de Minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de te bewaren gegevens per type van categorie bedoeld in de leden 1 tot 4 alsook de vereisten waaraan deze gegevens moeten beantwoorden.

§ 4. Wat betreft de bewaring van de gegevens bedoeld in paragraaf 3, dienen de aanbieders en operatoren beoogd in paragraaf 1, eerste lid:

1° te garanderen dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

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;

3° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de vragen van de autoriteiten bedoeld in paragraaf 2, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel

à l'exclusion des données prévues à l'alinéa 4, sont conservées op [9/12] mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, l'horodatage, l'identification des équipements terminaux à partir desquels ou vers lesquels des communications sont adressées ou ont été adressées, sont conservées op [9/12] mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 4 ainsi que les exigences auxquelles ces données doivent répondre.

§ 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs visés au paragraphe 1er, alinéa 1er :

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ;

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 ;

3° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er ;

126/1, § 1;

4° de gegevens op het grondgebied van de Europese Unie te bewaren;

4° conservent les données sur le territoire de l'Union européenne ;

5° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, van bij hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er inzage in te hebben;

5° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, incompréhensibles et inexploitables par toute personne qui n'est pas autorisée à y avoir accès ;

6° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt zoals vastgelegd in paragraaf 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123;

6° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123 ;

7° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit beoogd in paragraaf 2. Deze opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.

7° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2. Cette traçabilité s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.

De Koning bepaalt, na overleg in de Ministerraad, op voorstel van de Minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de inhoud van het logboek bedoeld in het tweede lid.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, le contenu du journal visé à l'alinéa 2.

§ 5. De minister en de Minister van Justitie zorgen ervoor dat statistieken inzake de bewaring van de gegevens die worden gegenereerd of behandeld in het kader van de verstrekking van openbaar toegankelijke communicatienetwerken en -diensten jaarlijks worden bezorgd aan de Kamer van volksvertegenwoordigers.

§ 5. Le ministre et le Ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Chambre des représentants.

Die statistieken omvatten met name:

Ces statistiques comprennent notamment :

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens

1° les cas dans lesquels des informations ont été transmises aux autorités compétentes

zijn verstrekt aan de bevoegde autoriteiten;

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

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

Deze statistische informatie mag geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, 1°, worden tevens bijgevoegd bij het verslag dat de Minister van Justitie overeenkomstig artikel 90decies van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de Minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, jaarlijks moeten bezorgen aan het Instituut en die welke het Instituut bezorgt aan de minister en aan de Minister van Justitie.

§ 6. Onverminderd het verslag bedoeld in paragraaf 5, vierde lid, brengen de minister en de Minister van Justitie, twee jaar na de inwerkingtreding van deze wet een evaluatieverslag uit over de toepassing van het koninklijk besluit bedoeld in paragraaf 3, vijfde lid, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn. "

Art. 5. In dezelfde wet wordt een artikel 126/1 ingevoegd, luidende:

§ 1. Binnen elke operator en elke aanbieder beoogd in artikel 126, § 1, eerste lid, wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde Belgische autoriteiten, op hun verzoek, van de gegevens bewaard krachtens de artikelen 122, 123 en 126, de identificatiegegevens van

conformément aux dispositions légales applicables ;

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

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

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, 1°, sont également jointes au rapport que le Ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du Ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au Ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, le ministre et le Ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 3, alinéa 5, sur la mise en œuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation. ».

Art. 5. Dans la même loi, un article 126/1 est inséré rédigé comme suit:

§ 1. Au sein de chaque opérateur, et au sein de chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est constituée une Cellule de coordination, chargée de fournir aux autorités belges légalement habilitées, à leur demande, des données conservées en vertu des articles 122, 123 et 126, les données d'identification de

de oproeper krachtens artikel 107, § 2, eerste lid, of de gegevens die kunnen vereist zijn krachtens de artikelen 46*bis*, 88*bis* en 90*ter* van het Wetboek van strafvordering en de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

l'appelant en vertu de l'article 107, § 2, alinéa 1er ou les données qui peuvent être requises en vertu des articles 46*bis*, 88*bis* et 90*ter* du Code d'instruction criminelle et des articles 18/7, 18/8, 18/16 et 18/17 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Desgevallend kunnen verscheidene operatoren of aanbieders een gemeenschappelijke Coördinatiecel oprichten. In een dergelijk geval moet deze Coördinatiecel voorzien in dezelfde dienst voor elke operator of aanbieder individueel.

Le cas échéant, plusieurs opérateurs ou fournisseurs peuvent créer une Cellule de coordination commune. En pareil cas, cette Cellule de coordination doit prévoir le même service pour chaque opérateur ou fournisseur individuel.

Om deel uit te maken van de Coördinatiecel dient voorafgaand te worden voldaan aan de volgende cumulatieve voorwaarden:

Afin de faire partie de la Cellule coordination, il faut au préalable répondre aux conditions cumulatives suivantes :

1° Het voorwerp hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies conform artikel 22*quinquies* van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Een advies wordt als achterhaald beschouwd 5 jaar na zijn verstrekking.

1° Avoir fait l'objet d'un avis de sécurité positif et non périmé conformément à l'article 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Un avis est considéré comme étant périmé 5 ans après son octroi.

2° Niet het voorwerp hebben uitgemaakt van een weigering door de Minister van Justitie, waarbij die weigering moet worden gemotiveerd en zich ten allen tijde kan voordoen.

2° Ne pas avoir fait l'objet d'un refus du Ministre de la Justice, ce refus devant être motivé et pouvant intervenir en tout temps.

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

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

De leden van de Coördinatiecel zijn onderworpen aan het beroepsgeheim.

Les membres de la Cellule de coordination sont soumis au secret professionnel.

Elke operator en elke aanbieder beoogd in artikel 126, § 1, eerste lid, waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel en

Chaque opérateur, et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, veille à la confidentialité des données traitées par la Cellule de coordination et communique sans

deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de Coördinatiecel en van zijn leden mee alsook elke wijziging van die gegevens.

délai à l'Institut et à la Commission pour la protection de la vie privée les coordonnées de la Cellule de coordination et de ses membres ainsi que toute modification de ces données.

§ 2. Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, stelt een interne procedure op om te antwoorden op de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens betreffende de gebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.

§ 2. Chaque opérateur, et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Elke operator en elke aanbieder beoogd in artikel 126, § 1, eerste lid, wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, voor de gegevens behandeld op basis van artikel 126 en dit artikel.

Chaque opérateur, et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est considéré comme responsable du traitement au sens 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 pour les données traitées sur base de l'article 126 et du présent article.

De operatoren van openbare netwerken voor elektronische communicatie en de aanbieders bedoeld in artikel 126, § 1, eerste lid, nemen artikel 114, § 2, in acht voor de toegang tot de gegevens bedoeld in paragraaf 1 en hun bezorging aan de autoriteiten.

Les opérateurs de réseaux publics de communications électroniques et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, respectent l'article 114, § 2, pour l'accès aux données visées au paragraphe 1er et leur transmission aux autorités.

§ 3. Elke aanbieder beoogd in artikel 126, § 1, eerste lid, en elke operator bedoeld in artikel 126, § 1, eerste lid, wijst een of meer aangestelden aan voor de bescherming van persoonsgegevens, die moet beantwoorden aan de cumulatieve voorwaarden opgesomd in paragraaf 1, derde lid. Deze aangestelde mag geen deel uitmaken van de Coördinatiecel.

§ 3. Chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, et chaque opérateur visé à l'article 126, § 1er, alinéa 1er, désigne un ou plusieurs préposés à la protection des données à caractère personnel, qui doit répondre aux conditions cumulatives énumérées au paragraphe 1er, alinéa 3. Ce préposé ne peut pas faire partie de la Cellule de coordination.

Bij de uitvoering van zijn opdrachten handelt de aangestelde voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid, en heeft hij toegang tot alle persoonsgegevens die worden bezorgd aan de autoriteiten, alsook tot alle relevante lokalen van de aanbieder of de operator.

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données à caractère personnel transmises aux autorités ainsi qu'à tous les locaux pertinents du fournisseur ou de l'opérateur.

De uitoefening van zijn opdrachten mag voor de aangestelde geen nadelen met zich brengen. Hij mag in het bijzonder als aangestelde niet worden ontslagen of vervangen wegens de uitvoering van de taken die hem zijn toevertrouwd, zonder grondige motivering.

L'exercice de ses missions ne peut entraîner pour le préposé des désavantages. Il ne peut, en particulier, être licencié ou remplacé comme préposé à cause de l'exécution des tâches qui lui sont confiées, sans motivation approfondie.

De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met het management of het directiecomité.

Le préposé doit avoir la possibilité de communiquer directement avec le management ou le comité de direction.

In het bijzonder zorgt de aangestelde voor de gegevensbescherming ervoor dat:

Le préposé à la protection des données veille à ce que :

1° de behandelingen door de Coördinatiecel worden uitgevoerd conform de wet;

1° les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi ;

2° de aanbieder of de operator enkel die gegevens verzamelt en bewaart die hij wettelijk mag bewaren;

2° le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver ;

3° enkel de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens;

3° seules les autorités légalement autorisées aient accès aux données conservées ;

4° de maatregelen voor beveiliging en bescherming van persoonsgegevens beschreven in deze wet en in het veiligheidsbeleid van de aanbieder of de operator ten uitvoer worden gebracht.

4° les mesures de sécurité et de protection des données à caractère personnel décrites dans la présente loi et dans la politique de sécurité du fournisseur ou de l'opérateur soient mises en œuvre.

Elke aanbieder bedoeld in artikel 126, § 1, eerste lid, en elke operator beoogd in artikel 126, § 1, eerste lid, deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de aangestelde(n) voor de bescherming van persoonsgegevens mee alsook elke wijziging van die gegevens.

Chaque fournisseur visés à l'article 126, § 1er, alinéa 1er, et chaque opérateur visé à l'article 126, § 1er, alinéa 1er, communique sans délai à l'Institut et à la Commission pour la protection de la vie privée les coordonnées du ou des préposés à la protection des données à caractère personnel, ainsi que toute modification de ces données.

§ 4. De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut:

§ 4. Le Roi détermine, par arrêté délibéré en Conseil des Ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut :

1° de categorieën van operatoren en de categorieën van aanbieders bedoeld in artikel

1° les catégories d'opérateurs et les catégories de fournisseurs visés à l'article 126, § 1er, alinéa

126, § 1, eerste lid, die zijn vrijgesteld van bepaalde eisen vastgelegd in paragraaf 1;

2° de nadere bepalingen van de aanvraag en de verstrekking van het veiligheidsadvies;

3° de vereisten waaraan de Coördinatiecel moet beantwoorden;

4° de categorieën van aanbieders bedoeld in artikel 126, § 1, eerste lid, en de categorieën van operatoren bedoeld in artikel 126, § 1, eerste lid, die zijn vrijgesteld van de naleving van een deel of van het geheel van paragraaf 3;

5° de informatie die moet worden verstrekt aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer conform de paragrafen 1 en 3 alsook de autoriteiten die toegang hebben tot die informatie;

6° de overige regels die de samenwerking van de operatoren en van de aanbieders bedoeld in artikel 126, § 1, eerste lid, met de Belgische autoriteiten of met sommige van hen, regelen, voor de verstrekking van de in paragraaf 1 beoogde gegevens."

Art. 6. In artikel 127 van dezelfde wet, gewijzigd door de wetten van 4 februari 2010, 10 juli 2012 en 27 maart 2014, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de volgende wijzigingen aangebracht:

a) in het eerste lid worden de woorden ",aan de aanbieders beoogd in artikel 126, § 1, eerste lid," ingevoegd tussen de woorden "aan de operatoren" en de woorden "of aan de eindgebruikers";

b) in het tweede lid worden de woorden "en de aanbieders beoogd in artikel 126, § 1, eerste lid," ingevoegd tussen de woorden "de operatoren" en de woorden "aan de operaties";

1er, qui sont dispensés de certaines exigences fixées au paragraphe 1er ;

2° les modalités de la demande et de l'octroi de l'avis de sécurité ;

3° les exigences auxquelles la Cellule de coordination doit répondre ;

4° les catégories de fournisseurs visés à l'article 126, § 1er, alinéa 1er, et les catégories d'opérateurs visés à l'article 126, § 1er, alinéa 1er, qui sont dispensés du respect du paragraphe 3, en tout ou en partie ;

5° les informations à fournir à l'Institut et à la Commission pour la protection de la vie privée conformément aux paragraphes 1 et 3 ainsi que les autorités qui ont accès à ces informations ;

6° les autres règles régissant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er avec les autorités belges ou avec certaines d'entre elles, pour la fourniture des données visées au paragraphe 1er. ».

Art. 6. Dans l'article 127 de la même loi, modifié par les lois des 4 février 2010, 10 juillet 2012 et 27 mars 2014, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots « , aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, » sont insérés entre les mots « aux opérateurs » et les mots « ou aux utilisateurs finals » ;

b) dans l'alinéa 2, les mots « et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, » sont insérées entre les mots « des opérateurs » et les mots « aux opérations » ;

2° paragraaf zes wordt opgeheven.

2° le paragraphe 6 est abrogé.

Art. 7. In artikel 145, § 1, van dezelfde wet, gewijzigd door de wetten van 25 april 2007 en 27 maart 2014 worden de volgende wijzigingen aangebracht:

Art. 7. Dans l'article 145, § 1er, de la même loi, modifié par les loi du 25 avril 2007 et du 27 mars 2014, les modifications suivantes sont apportées :

1° de woorden "126, 126/1," worden ingevoegd tussen de woorden "124," en "127";

1° les mots « 126, 126/1, » sont insérés entre les mots « 124, » et le mot « 127 » ;

2° de woorden ",126, 126/1" worden ingevoegd tussen de woorden "47" en "en 127";

2° les mots « ,126, 126/1 » sont insérés entre entre les mots « 47 » et « et 127 » ;

3° het artikel wordt aangevuld met een paragraaf 3*ter* luidend als volgt:

3° l'article est complété par le paragraphe 3*ter* rédigé comme suit :

" § 3ter. 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:

« § 3*ter*. Est puni d'une amende de 50 euros à 50.000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :

1° 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 gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;

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 visées à l'article 126 ;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, 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, ou les divulgue ou fait un usage quelconque des données ainsi obtenues. ».

HOOFDSTUK 3. - Bepalingen tot wijziging van het Wetboek van strafvordering	CHAPITRE 3. – Dispositions modifiant le Code d'instruction criminelle
Art. 8. In artikel 46bis, § 1, van het Wetboek van strafvordering, ingevoegd bij de wet van 10 juni 1998 en gewijzigd bij de wetten van 27 december 2004 en 23 januari 2007, wordt een vierde lid toegevoegd, luidend als volgt:	Art. 8. A l'article 46bis, § 1er, du Code d'instruction criminelle, inséré par la loi du 10 juin 1998 et modifié par les lois du 27 décembre 2004 et 23 janvier 2007, un alinéa 4 est ajouté, libellé comme suit :
"Voor strafbare feiten die een correctionele hoofdgevangenisstraf van minder dan één jaar tot gevolg kunnen hebben, kan de procureur des Konings de in het eerste lid bedoelde gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing."	« Pour des infractions qui peuvent donner lieu à une peine d'emprisonnement correctionnel principal de moins d'un an, le procureur du Roi ne peut requérir les données visées au premier alinéa que pour une période de six mois préalable à sa décision. »
Art. 9. In artikel 88bis van hetzelfde Wetboek, ingevoegd door de wet van 11 februari 1991 en gewijzigd bij de wetten van 30 juni 1994, 10 juni 1998, 8 juni 2008 en 27 december 2012, worden de volgende wijzigingen aangebracht:	Art. 9. A l'article 88bis du même Code, inséré par la loi du 11 février 1991 et modifié par les lois du 30 juin 1994, 10 juin 1998, 8 juin 2008 et du 27 décembre 2012, les modifications suivantes sont apportées :
1° In § 1 wordt het eerste lid vervangen als volgt:	1° Au § 1er, l'alinéa 1er est remplacé comme suit :
"Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij, zo nodig door daartoe rechtstreeks of via de door de Koning aangewezen politiedienst de medewerking van de operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst te vorderen:	«S'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique:
1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;	1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressés ou ont été adressés ;

2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren.”

2° à la localisation de l'origine ou de la destination de communications électroniques. »

2° In § 1, tweede lid wordt het woord “telecommunicatiemiddel” vervangen door de woorden “elektronisch communicatiemiddel” en het woord “telecommunicatie” door het woord “elektronische communicatie”.

2° Au §1er, alinéa 2, les mots « moyen de télécommunication » sont remplacés par les mots « moyen de communication électronique » et les mots « de la télécommunication » par les mots « de la communication électronique ».

3° In § 1 wordt het derde lid vervangen als volgt:

3° Au §1er, l’alinéa 3 est remplacé comme suit :

“De onderzoeksrechter doet in een gemotiveerd bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.”

« Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée. »

4° § 1 wordt het vierde lid vervangen als volgt:

4° § 1er, alinéa 4, est remplacé par :

“Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig § 2.”

« Il précise la durée durant laquelle elle pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l’ordonnance s’étend conformément au § 2. »

5° § 1 wordt aangevuld met een zevende lid, luidend als volgt:

5° le § 1er est complété par un alinéa 7 rédigé comme suit :

“In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde en vierde lid.”

« En cas d’urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 3 et 4. ».

6° Er wordt een § 2 ingevoegd, luidend als volgt:

6° Un § 2 est inséré, libellé comme suit :

“§ 2. Wanneer de maatregel bedoeld in § 1 betrekking heeft op verkeers- of lokalisatiegegevens van elektronische communicatiemiddelen van waaruit of

« § 2. Lorsque la mesure visée au § 1er concerne des données de trafic ou de localisation de moyens de communication électronique à partir desquels ou vers lesquels

waarnaar elektronische communicaties werden gedaan, zijn de volgende bepalingen van toepassing:

- Voor strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, of die gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324bis van het Strafwetboek, of die een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens bedoeld in § 1, eerste lid, die op basis van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie bewaard worden, vorderen voor een periode van op [9/12] maanden voorafgaand aan het bevelschrift;

  In dit geval kan de onderzoeksrechter in hetzelfde bevelschrift de gegevens vorderen die op basis van andere wettelijke bepalingen bewaard worden, voor een periode die langer is dan de periode van op [9/12] maanden. Hij dient dit uitdrukkelijk aan te geven in zijn bevelschrift.

- Voor andere strafbare feiten kan de onderzoeksrechter de gegevens bedoeld in § 1, eerste lid, die op basis van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie bewaard worden slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift. Hij kan geen andere gegevens vorderen".

des communications électroniques ont été adressés, les dispositions suivantes s'appliquent :

- Pour des infractions comme visées à l'article 90ter, §§ 2 à 4, ou qui sont commises dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou qui sont de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données visées au § 1er, alinéa 1er, qui sont conservées sur base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, pour une période de [9/12] mois préalable à l'ordonnance.

  Dans ce cas, le juge d'instruction peut requérir dans la même ordonnance les données qui sont conservées sur la base d'autres dispositions légales, pour une période plus longue que la période de op [9/12] mois. Il doit l'indiquer expressément dans son ordonnance.

- Pour d'autres infractions, le juge d'instruction ne peut requérir les données visées au § 1er, alinéa 1er, qui sont conservées sur base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, que pour une période de six mois préalable à l'ordonnance. Il ne peut pas requérir des autres données. »

7° Er wordt een § 3 ingevoegd, luidend als volgt:

"§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in § 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 § 1 te

7° Un § 3 est inséré, libellé comme suit :

« § 3. La mesure ne pourra 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 des infractions visées au § 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées au § 1er, utilisent ses moyens de communication

hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. Diezelfden 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."

8° In § 2, die tot § 4 vernummerd wordt, worden in het eerste lid de woorden "Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst" vervangen door de woorden "Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst".

Art. 10. Artikel 90decies van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002 en 6 januari 2003, wordt aangevuld met een lid, luidende:

"Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 5, vierde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. ".

Hoofdstuk IV. Bepalingen tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 11. In artikel 13 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, gewijzigd door de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht:

1° In het eerste lid wordt het woord "inlichtingen" vervangen door het woord "informatie".

2° Het derde lid wordt vervangen als volgt:

électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne seront pas consignés au procès-verbal. »

8° Au § 2, qui devient § 4, à l'alinéa 1er, les mots « Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication » sont remplacé par les mots « Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique ».

Art. 10. L'article 90decies du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois du 8 avril 2002, 7 juillet 2002 et du 6 janvier 2003, est complété par un alinéa, rédigé comme suit :

« A ce rapport est joint le rapport dressé en application de l'article 126, § 5, alinéa 4, de la loi du 13 juin 2005 relative aux communications électroniques. »

Chapitre IV. Dispositions modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 11. À l'article 13 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, telle que modifiée par la loi du 4 février 2010, les modifications suivantes sont apportées :

1° Dans le texte néerlandais de l'alinéa premier, le mot «inlichtingen» est remplacé par le mot «informatie».

2° Le troisième alinéa est remplacé comme

	suit:
“De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en over de informatie en persoonsgegevens die zij leveren.”	“Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et aux informations et données à caractère personnel qu'elles fournissent.”
3° Er wordt een vierde lid ingevoegd, luidend als volgt:	**3°** Un quatrième alinéa est inséré, libellé comme suit :
“De agenten van de inlichtingen- en veiligheidsdiensten hebben toegang tot de door hun dienst ingewonnen en verwerkte informatie, inlichtingen en persoonsgegevens, voor zover deze nuttig zijn voor de uitoefening van hun functie of opdracht.”	« Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission. »
Art. 12. In artikel 18/3 van de wet van 30 november 1998, ingevoegd door de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht:	Art. 12. À l’article 18/3 de la loi du 30 novembre 1998, inséré par la loi du 4 février 2010, les modifications suivantes sont apportées :
1° Er wordt een §2 ingevoegd, luidend als volgt:	**1°** Un §2 est inséré, libellé comme suit:
“§2. De beslissing van het diensthoofd vermeldt: 1° de aard van de specifieke methode; 2° naargelang het geval, de natuurlijke pers(o)n(en) of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode; 3° de potentiële bedreiging die de specifieke methode rechtvaardigt; 4° de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen 2° en 3°; 5° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de BIM-Commissie; 6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen ; 7° in voorkomend geval, het technisch hulpmiddel dat gebruikt wordt bij de aanwending van de specifieke methode; 8° in voorkomend geval, de samenloop met een	“§2. La décision du dirigeant du service mentionne: 1° la nature de la méthode spécifique ; 2° selon le cas, la ou les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique ; 3° la menace potentielle qui justifie la méthode spécifique ; 4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ; 5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission ; 6° le nom du (ou des) officier(s) de renseignement responsable(s) pour le suivi de la mise en œuvre de la méthode spécifique ; 7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode spécifique; 8° le cas échéant, le concours avec une information ou une instruction judiciaire ; 9° le cas échéant, les indices sérieux attestant que l’avocat, le médecin ou le journaliste participe ou a participé personnellement et

opsporings- of gerechtelijke onderzoek;
9° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële bedreiging;
10° in geval toepassing wordt gemaakt van artikel 18/8, de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft;
11° de datum van de beslissing;
12° de handtekening van het diensthoofd."

activement à la naissance ou au développement de la menace potentielle ;
10° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données ;
11° la date de la décision ;
12° la signature du dirigeant du service."

2° §3 wordt vervangen door het eerste lid van §2 en wordt aangevuld met een tweede lid, luidende als volgt:
"Deze lijsten bevatten de gegevens bedoeld in § 2, 1° à 3°, 5° en 7°.".

2° Le §3 est remplacé par l'alinéa 1er du §2 et est complété par un deuxième alinéa rédigé comme suit :
« Ces listes comprennent les données visées au § 2, 1° à 3°, 5° et 7°. ».

3° §2, tweede tot vijfde lid wordt vernummerd tot §6.

3° Le §2, alinéas 2 à 5 est renuméroté §6.

4° Het derde lid van §1 wordt vernummerd naar §5.

4° Le troisième alinéa du § 1er est renuméroté §5.

5° Het vierde lid van §1 wordt vernummerd naar §7 en de woorden "om de specifieke methode voor het verzamelen van gegevens aan te wenden" worden vervangen door de woorden "om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen".

5° Le quatrième alinéa du § 1er est renuméroté §7 et le terme « mettre » est remplacé par les termes « le suivi de la mise ».

6° Er wordt een §8 ingevoegd, luidend als volgt:

"§8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële bedreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie."

6° Un §8 est inséré, libellé comme suit :

"§8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la Commission de sa décision."

Artikel 13

In artikel 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, gewijzigd door de wet van 4 februari 2010, worden de volgende

Article 13

A l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, modifiée par la loi du 4 février 2010, les modifications suivantes sont apportées :

wijzigingen aangebracht:

1° In § 1 wordt het eerste lid vervangen als volgt:

“De inlichtingen- en veiligheidsdiensten kunnen, wanneer dit een belang vertoont voor de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.”

1° Au § 1er, l’alinéa premier est remplacé comme suit :

"Les services de renseignement et de sécurité peuvent, si cela présente un intérêt pour l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique, procéder ou faire procéder :

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

2° à la localisation de l'origine ou de la destination de communications électroniques."

2° In § 1, tweede lid, wordt het woord “oproepgegevens” vervangen door het woord “verkeersgegevens”.

2° Au § 1er, alinéa 2, les mots “données d'appel” sont remplacés par les mots “données de trafic”.

3° Er wordt een §2 ingevoegd, luidend als volgt:

“§2. Wanneer de methode bedoeld in §1 betrekking heeft op verkeers- of lokalisatiegegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties werden gedaan, zijn de volgende bepalingen van toepassing:

a) Voor een potentiële bedreiging zoals bedoeld in artikel 18/1, andere dan deze bedoeld in b), kan het diensthoofd in zijn beslissing de gegevens bedoeld in § 1, eerste lid, die op basis van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie bewaard worden, vorderen voor een periode van [twaalf] maanden voorafgaand aan de beslissing.

In dit geval kan het diensthoofd in dezelfde beslissing de gegevens vorderen die op basis van andere wettelijke bepalingen bewaard

3° Il est inséré un §2, libellé comme suit :

“§2. Lorsque la méthode visée au § 1er concerne des données de trafic ou de localisation de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques ont été adressés, les dispositions suivantes s’appliquent :

a) Pour une menace potentielle telle que visée à l'article 18/1, autre que celles visées sous b), le dirigeant du service peut dans sa décision requérir les données visées au § 1er, alinéa 1er, qui sont conservées sur base de l’article 126 de la loi du 13 juin 2005 relative aux communications électroniques, pour une période de [douze] mois préalable à la décision.

Dans ce cas, le dirigeant du service peut requérir dans la même décision les données qui sont conservées sur la base d’autres

worden, voor een periode die langer is dan de periode van [twaalf] maanden. Hij dient dit uitdrukkelijk aan te geven in zijn beslissing.

b) Voor een potentiële bedreiging die betrekking heeft op een activiteit die verband kan houden met inmenging, criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd de gegevens bedoeld in § 1, eerste lid, die op basis van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie bewaard worden, slechts vorderen voor een periode van [zes] maanden voorafgaand aan de beslissing. Hij kan geen andere gegevens vorderen."

4° §2 wordt vernummerd tot §4.

Gegeven te, …

dispositions légales, pour une période plus longue que la période de [douze] mois. Il doit l'indiquer expressément dans sa décision.

b) Pour une menace potentielle qui se rapporte à une activité qui peut être liée à l' ingérence, des organisations criminelles ou des organisations sectaires nuisibles, le dirigeant du service ne peut requérir les données visées au § 1er, alinéa 1er, qui sont conservées sur base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, que pour une période de [six] mois préalable à la décision. Il ne peut requérir aucune autre donnée."

4° Le §2 est renuméroté en §4.

Donné à …

Van Koningswege :

De Minister van Justitie,

Par le Roi :

Le Ministre de la Justice,

K. GEENS

De Minister van Digitale Agenda, Telecommunicatie en Post

Le Ministre de l'Agenda numérique, des Télécommunications et de la Poste

Alexander De Croo

De Minister van Defensie, Le Ministre de la Défense,

Steven VANDEPUT