DOC 54 **1567/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

11 januari 2016

WETSONTWERP

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

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

11 janvier 2016

PROJET DE LOI

relatif à la collecte et à la conservation des données dans le secteur des communications électroniques

Blz.

INHOUD

Pages

SOMMAIRE

OVEREENKOMSTIG ARTIKEL 8, § 2, 1°, VAN DE WET VAN 15 DECEMBER 2013 WERD DE IMPACTANALYSE NIET GEVRAAGD.

CONFORMÉMENT À L'ARTICLE 8, § 2, 1°, DE LA LOI DU 15 DÉCEMBRE 2013, L'ANALYSE D'IMPACT N'A PAS ÉTÉ DEMANDÉE.

De regering heeft dit wetsontwerp op 11 januari 2016 ingediend.	*Le gouvernement a déposé ce projet de loi le 11 janvier 2016.*
De "goedkeuring tot drukken" werd op 21 januari 2016 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 21 janvier 2016.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*

Afkortingen bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*	*DOC 54 0000/000:*	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Schriftelijke Vragen en Antwoorden*	*QRVA:*	*Questions et Réponses écrites*
CRIV:	*Voorlopige versie van het Integraal Verslag*	*CRIV:*	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Beknopt Verslag*	*CRABV:*	*Compte Rendu Analytique*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*	*CRIV:*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Plenum*	*PLEN:*	*Séance plénière*
COM:	*Commissievergadering*	*COM:*	*Réunion de commission*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT:*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

SAMENVATTING

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.

Het behoudt in de wet betreffende de elektronische communicatie voor de operatoren opnieuw de verplichting in om bepaalde gegevens betreffende de communicaties te bewaren, maar met wijzigingen.

Het wijzigt het Wetboek van Strafvordering en de wet houdende regeling van de inlichtingen- en veiligheidsdienst door de waarborgen inzake de toegang tot de gegevens te versterken.

RÉSUMÉ

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.

Il réintroduit dans la Loi sur les communications électroniques l'obligation pour les opérateurs de conserver certaines données relatives aux communications mais avec des modifications.

Il modifie le code d'instruction criminelle et la loi organique relative aux services de renseignement et de sécurité en renforçant les garanties concernant l'accès aux données.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

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.

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 artikelen 122 en 123 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).

EXPOSE DES MOTIFS

MESDAMES, MESSIEURS,

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. **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 les articles 122 et 123 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).

Het wetsontwerp verkreeg een gunstig advies van de Commissie voor de bescherming van het privéleven (advies 33-2015 van 9 september 2015).

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 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 en de verscheidenheid aan communicaties, zulks ondanks de eveneens groeiende bekommernis inzake de persoonlijke levenssfeer.

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.

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

De sector van het terrorisme is uiteraard bijzonder actueel. De toegang tot de communicatiegegevens

Le projet de loi a fait l'objet d'un avis favorable de la Commission pour la protection de la vie privée (avis 33-2015 du 9 septembre 2015).

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 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 et de la diversité des communications même si la préoccupation en matière de vie privée va également croissant.

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.

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

Le secteur du terrorisme est évidemment particulièrement d'actualité. L'accès aux données de

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.

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 criminele 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;

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'ensuit 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.

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 criminel.

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;

— 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.

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.

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

— 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 États-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.

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. **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

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 toegang zal bovendien steeds beperkt zijn in de tijd, met een maximum van 12 maanden.

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.

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"). Artikel 123 WEC staat overigens de verwerking van de locatiegegevens toe zolang de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens.

Het lijdt echter geen twijfel dat de gegevens die de operatoren bewaren op grond van de artikelen 122 en 123 WEC gedurende heel deze bewaring 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. Het wetsontwerp wijzigt op dat punt niets aan de situatie en kan niet worden geïnterpreteerd als een beperking van de toegang of de duur van de toegang tot de gegevens die worden bewaard op basis van deze artikelen 122 en 123 WEC.

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, die afwijken van de facturatie

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.

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.

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"). L'article 123 LCE permet par ailleurs le traitement des données de localisation tant que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation.

Or il ne fait pas de doute que les données conservées par les opérateurs sur base des articles 122 et 123 LCE peuvent être tout au long de cette conservation utilisées pour les finalités de l'enquête pénale ou du renseignement, dans les conditions prévues par ces cadres légaux. Le projet de loi ne modifie aucunement la situation à cet égard et ne saurait être interprété comme restreignant l'accès ou la durée d'accès aux données conservées sur base de ces articles 122 et 123 LCE.

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*", qui s'écartent de la facturation à l'usage, certaines données jusqu'alors

voor effectief verbruik, 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.

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.

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 het stelselmatige gebruik van hun gegevens door private actoren voor commerciële doeleinden.

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

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.

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.

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'État. 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 à l'utilisation systématique de leurs données par des acteurs privés pour des motifs commerciaux.

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 l'accès des autorités aux données concernées;

— 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.

De Commissie is dezelfde mening toegedaan, aangezien zij er in voormeld advies 33-2015 op wijst dat "bepaalde aspecten van [de] arresten [van het Hof van justitie en het grondwettelijke Hof] de Commissie evenwel moeilijk toepasbaar [lijken] te zijn, in het bijzonder het onderscheid op grond van personen, periodes en/of geografische zones"

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.

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

— 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.

Dans l'avis 33-2015 précité, la Commission va dans le même sens puisqu'elle indique que "certains aspects des arrêts [de la Cour de justice et de la Cour constitutionnelle] lui paraissent difficilement applicables, en particulier la distinction en fonction des personnes, périodes temporelles et/ou zones géographiques".

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.

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,

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 décharge kan meespelen.

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 (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).

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) 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 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.

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”.

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.

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.

Verder in de tekst zal evenwel blijken dat 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.

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.

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

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) 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”.

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.

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.

On verra toutefois plus loin que la protection de certaines professions est bien renforcée dans le présent projet de loi mais au niveau de la réglementation de l’accès aux données conservées.

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.

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

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.

In voormeld advies over onderhavig wetsontwerp steunt de Commissie deze interpretatie en stelt ze: “evenwel wordt, zoals de Memorie van toelichting aangeeft, in geen van beide arresten geconcludeerd dat slechts één van de vier elementen volstaat om een schending van het evenredigheidsbeginsel in te houden. Indien een bepaald element van de arresten niet kan worden weerhouden, dient dit gecompenseerd te worden door een striktere regeling inzake de andere aspecten.”

8. **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”.

Dit ontwerp van wet voert een onderscheid in op grond van drie categorieën van gegevens.

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, worden het meest gevraagd en tasten de persoonlijke levenssfeer op matige wijze aan, in vergelijking met inzonderheid de tweede en derde categorie.

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

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

De tweede en derde categorie tasten de persoonlijke levenssfeer meer aan dan de eerste. De toegangen tot die gegevens zijn minder talrijk dan die tot de identificatiegegevens maar blijven frequent.

Na veelvuldige besprekingen in de Regering en met de diensten en overheden in kwestie, en na een differentiatie in de bewaringstermijnen overwogen te hebben in functie van de categorieën van gegevens, is de conclusie dat, gelet op de noodwendigheden inzake de strijd tegen terroristische misdrijven, een

examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.

Dans son avis précité sur le présent projet de loi, la Commission vie privée soutient cette interprétation et indique: “comme indiqué dans l’Exposé des Motifs, aucun des deux arrêts ne conclut qu’un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects.”

8. **Les 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”.

Le présent projet de loi introduit une distinction sur base de 3 catégories de données.

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 sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux deuxième et troisième catégories.

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

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

Les deuxième et troisième catégories sont plus attentatoires à la vie privée que la première. Les accès à ces données sont moins nombreux que ceux aux données d’identification mais restent fréquents.

Après de nombreuses discussions au sein du gouvernement et avec les services et autorités concernées, et après avoir envisagé une différenciation entre les délais de conservation en fonction des catégories de données, la conclusion est que, vu les nécessités liées à la lutte contre les infractions terroristes, une période de

bewaringsperiode van 12 maanden noodzakelijk is voor elk van de 3 categorieën.

9. **Versterking van de garanties op het niveau van 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 46*bis* en 88*bis* van het Wetboek van strafvordering voor het strafrechtelijke kader en de artikelen 18/7 en 18/8 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 identificatiegegevens die wordt geregeld in artikel 46*bis* van het Wetboek van strafvordering en die betrekking heeft op de toegang tot de gegevens van de eerste twee categorieën. Dat artikel 46*bis* 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

12 mois de conservation est nécessaire pour chacune des 3 catégories.

9. **Le renforcement des garanties au niveau 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 46*bis* et 88*bis* du Code d'instruction criminelle pour le cadre pénal et les articles 18/7 et 18/8 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 qui est réglé par l'article 46*bis* du Code d'instruction criminelle et qui concerne l'accès aux données des deux premières catégories. Cet article 46*bis* 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

persoonlijke levenssfeer beperkt blijft. De voorwaarden blijven uiteraard van toepassing, inzonderheid de voorafgaande en gemotiveerde instemming van het parket of van de onderzoeksrechter.

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

De Raad van State merkt op in zijn advies dat dit niet dezelfde differentiatie op grond van de ernst van het misdrijf is als deze voorzien voor artikel 88*bis* Sv. (zie *infra*), en dat de redenen hiervoor duidelijker moeten worden aangegeven.

Vooreerst zou het onredelijk zijn om het opvragen van de gegevens bedoeld in artikel 46*bis*, § 1, 1° en 2°, enkel mogelijk te maken voor zware misdrijven.

Zoals reeds gezegd, zijn de bedoelde identificatiegegevens niet van die aard dat de mededeling ervan een verregaande inbreuk op het privéleven inhoudt.

Tenslotte gaat de redenering van de Raad van State slechts ten dele op, waar hij stelt dat de identificatiegegevens van artikel 46*bis de facto* gedurende een veel langere termijn bewaard kunnen blijven dan twaalf maanden. Enerzijds klopt het dat deze bewaartermijn pas aanvangt “de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst” (artikel 126, § 3, eerste lid WEC), maar anderzijds zal deze regel in de praktijk niet altijd leiden tot een langere bewaartermijn dan twaalf maanden.

Er moet inzonderheid rekening worden gehouden met het geval van de dynamische IP-adressen die regelmatig wijzigen en waarvoor de termijn begint te lopen vanaf het einde van de betrokken communicatie. Daarnaast wordt het, wegens de ontwikkelingen op het vlak van communicatie, steeds belangrijker om tijdens de onderzoeken te kunnen bepalen wie een specifiek IP-adres op tijdstip X gebruikte.

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 (verbindings- en lokalisatiegegevens en persoonlijke communicatiegegevens) wordt ook aanzienlijk versterkt op het stuk van de garanties. Die regeling wordt bepaald in artikel

entendu applicables, notamment l’autorisation préalable et motivée du parquet ou du juge d’instruction.

Le projet introduit néanmoins une différenciation de l’accès aux donnés à l’article 46*bis*, en ajoutant au § 1er que pour des infractions de moindre gravité, qui ne sont pas de nature à entraîner une peine d’emprisonnement correctionnel principal d’un an ou une peine plus lourde, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

Le Conseil d’État fait remarquer dans son avis que ce n’est pas la même différenciation sur base de la gravité de l’infraction que celle prévue pour l’article 88*bis* C.I.Cr. (voy. *infra*) et que les raisons y afférentes doivent être indiquées plus clairement.

Tour d’abord, il serait déraisonnable de rendre la demande des données visées à l’article 46*bis*, § 1, 1° et 2° possible seulement pour les infractions graves.

Comme il a déjà été indiqué, les données d’identification visées ne sont pas de nature à ce que leur communication implique une intrusion importante dans la vie privée.

Enfin, le raisonnement du Conseil d’État n’est que partiellement valide lorsqu’il indique que les données d’identification de l’article 46*bis* peuvent *de facto* être conservées pour une durée beaucoup plus longue que 12 mois. D’une part, il est vrai que ce délai de conservation ne commence à courir qu’à “la date à partir de laquelle une communication est possible pour la dernière fois à l’aide du service utilisé” (article 126, § 3, premier alinéa LCE) mais, d’autre part, cette règle ne va pas toujours mener dans la pratique à une durée de conservation plus longe que douze mois.

Il faut en particulier prendre en compte la situation des adresses IP dynamiques qui changent fréquemment et pour lesquelles le délai commencera à courir à partir de la fin de la communication concernée. Or, pouvoir identifier qui utilisait une adresse IP précise à un moment X est de plus en plus important pour les enquêtes en raison de l’évolution des communications.

Le régime applicable pour ce qui concerne le repérage des communications et donc l’accès aux données des deux dernières catégories (données de connexion et de localisation et données personnelles de communication) est également considérablement renforcé sur le plan des garanties. Ce régime est défini à l’article

88*bis* van het Wetboek van strafvordering. Het ontwerp van wet brengt drie hoofdgaranties aan.

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

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 minstens vijf jaar gevangenisstraf en/of die zijn opgenomen op de lijst waarin is voorzien in artikel 90*ter* van het Wetboek van strafvordering (met andere woorden de misdrijven die aanleiding kunnen geven tot telefoontap), en/of die gepleegd zijn in het kader van een criminele organisatie, kan de maatregel betrekking hebben op een periode van negen maanden voorafgaand aan het verzoek. Tenslotte kan ze betrekking hebben op de volledige bewaarperiode voor de onderzoeken inzake terrorisme.

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

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

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 is reeds grondig gereglementeerd.

Artikel 18/3 regelt de procedure voor de aanwending van de specifieke methoden en de controle erop door een onafhankelijke commissie, samengesteld uit drie magistraten (BIM-commissie). Het artikel voorziet eveneens in garanties met het oog op de vrijwaring van het beroepsgeheim van de advocaten en artsen en het bronnengeheim van de journalisten.

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);

88*bis* du Code d'instruction criminelle. Le projet de loi apporte trois garanties principales.

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.

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 d'au moins cinq ans d'emprisonnement et/ou reprises sur la liste prévue à l'article 90*ter* du Code d'instruction criminelle (c'est-à-dire les infractions pouvant donner lieu à écoute téléphonique), et/ou qui sont commises dans le cadre d'une organisation criminelle, la mesure pourra porter sur une période de neuf mois précédant la demande. Enfin, elle pourra porter sur l'entièreté de la période de conservation pour les enquêtes en matière de terrorisme.

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

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

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.

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

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);

— 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.

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

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.

Het is voor de inlichtingendiensten verboden om gegevens die worden beschermd door het 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.

In dit geval zijn er drie garanties voorzien:

— 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.

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.

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

— 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.

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

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.

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 sauf 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.

Dans ce cas, trois garanties sont prévues:

— 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.

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.

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

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, via de door de Koning aangewezen politiedienst, 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.

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 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.

11. **Situatie in de andere lidstaten**

Een samenvatting van de situatie in de volgende landen is in bijlage. 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

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, par l'intermédiaire d'un service de police désigné par le Roi, 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.

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 veiller au respect des différentes règles en la matière.

11. **La situation dans les autres États membres**

Un résumé de la situation dans les pays suivants est joint en annexe. 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, au Royaume-uni et en Autriche mais que les gouvernements allemands et néerlandais ont d'ores

een ontwerp van wet hebben goedgekeurd op grond waarvan het beginsel opnieuw wordt ingevoerd. De Britse regering staat erop de “data retention” te behouden en voorziet de invoering van een beroep tegen de vernietigingsbeslissing die nog niet uitvoerbaar is. 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. Enkel Luxemburg heeft zijn wetgeving op bepaalde punten aangepast.

12. **Advies van de Raad van State**

Tenslotte worden hierna enkele punten opgesomd waarvoor het advies nr. 58 449/4 van de afdeling wetgeving van de Raad van State niet kon worden gevolgd.

1. ***Kortere bewaartermijnen, met een activatie van langere termijnen in het geval van een dreiging***

De Raad van State stelt de vraag of het niet mogelijk is om te voorzien in een kortere algemene bewaartermijn van de gegevens, met de mogelijkheid een langere bewaartermijn te laten “activeren” door de Koning in welbepaalde omstandigheden van potentiële dreiging.

Voor die oplossing is niet geopteerd, omdat sommige gegevens dan niet meer beschikbaar zullen zijn op het moment van de effectieve activering van een langere bewaartermijn. Het is net in imminente dreigingssituaties dat het noodzakelijk is om de langst periode in de tijd terug te gaan om gegevens op te vragen.

2. ***De reglementering van het verzoek gericht aan de operatoren***

Betreffende de toegang tot de nooddiensten die hulp bieden ter plaatse, van de Ombudsdienst voor de telecommunicatie en van de cel Vermiste Personen van de federale politie tot bepaalde bewaarde data, vraagt de Raad van State zich af wat de nadere bepalingen zijn van het verzoek gericht aan de operatoren teneinde onregelmatige of onrechtmatige verzoeken te vermijden.

Het advies van de Raad van State werd gevolgd, behalve wat betreft het feit dat artikel 126/1, § 4, 4°, voorziet in de mogelijkheid voor de Koning om de vorm en de inhoud van het verzoek vast te leggen en verplicht dus niet om dat aspect te regelen.

et déjà adopté un projet de loi réintroduisant le principe. Le gouvernement britannique insiste sur le maintien de la “data retention” et prévoit d’introduire un recours contre la décision d’annulation qui n’est pas encore exécutoire. Les 5 autres États ont maintenu le principe dans leur droit national. Parmi ces États, 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. Seul le Luxembourg a entrepris l’adaptation de sa législation sur certains points.

12. **Avis du Conseil d’État**

Enfin, on reprend ci-après quelques points sur lesquels l’avis nr. 58 449/4 de la Section de législation du Conseil d’État n’a pas pu être suivi.

1. ***Des délais de conservation plus courts, avec une activation de délais plus longs en cas de menace***

Le Conseil d’État se demande s’il n’est pas possible de prévoir un délai de conservation des données général plus court, avec la possibilité de faire “activer” un délai de conservation plus long par le Roi dans des circonstances bien définies de menace potentielle.

Cette solution n’est pas choisie car certaines données ne seront alors plus disponibles au moment de l’activation effective d’un délai de conservation plus long. C’est justement dans des situations de menace imminente qu’il est nécessaire de revenir durant la période la plus longue dans le passé pour requérir les données.

2. ***La réglementation de la demande adressée aux opérateurs***

Concernant l’accès des services d’urgence offrant de l’aide sur place, du Service de médiation pour les télécommunications et de cellule de disparition de la police fédérale à certaines données conservées, le Conseil d’État se pose la question des modalités de la demande adressée aux opérateurs, afin d’éviter des demandes irrégulières ou abusives.

L’avis du Conseil d’État a été suivi, sauf concernant le fait que l’article 126/1, § 4, 4° prévoit la possibilité pour le Roi de fixer la forme et le contenu de la demande et ne l’oblige donc pas à réglementer cet aspect.

Er werd immers niet vastgesteld dat er zich momenteel moeilijkheden voordoen of dat de huidige reglementering en de delegaties aan de Koning waarin artikel 126/1 voorziet, ontoereikend zouden zijn. De vorm en de inhoud vastleggen van de verzoeken houdt overigens het risico in dat een zware en ondoeltreffende administratieve last wordt opgelegd aan de betrokken operatoren en overheden.

a) Het verzoek vanwege de nooddiensten:

Momenteel beschikken de nooddiensten die ter plaatse hulp bieden niet over een rechtstreekse telefoonlijn naar de operatoren om identificatiegegevens van de oproeper te vragen die de operator die is betrokken bij de noodoproep hen niet heeft verstrekt zoals hij hoort te doen conform artikel 107, § 2, van de WEC. Ze moeten dus dezelfde communicatiekanalen aanwenden als deze gebruikt door de bevolking om de operator te contacteren, wat nog benadrukt hoe belangrijk het is dat de operator zich ervan vergewist dat de oproep wel degelijk afkomstig is van de nooddiensten. Artikel 126/1 van het wetsontwerp voert evenwel de "Coördinatiecel" in binnen de operatoren en aanbieders, waartoe de nooddiensten toegang zullen hebben. Het is in het uitvoeringsbesluit van dat artikel dat aandacht zal moeten worden besteed aan de veiligheidsmechanismen van de verzoeken om en overdracht van informatie, bijvoorbeeld door de operatoren te verplichten om het (niet-openbare) nummer van de rechtstreekse telefoonlijn van de Coördinatiecel mee te delen aan de nooddiensten die ter plaatse hulp bieden. Dat zal mogelijk zijn wanneer de tekst van artikel 126/1, § 4, 3°, de Koning de bevoegdheid geeft om "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" vast te leggen en paragraaf 1 van artikel 126/1 onder andere voorziet in de melding aan de Commissie voor de bescherming van de persoonlijke levenssfeer en aan het BIPT van de contactgegevens van de "Coördinatiecel". Deze eerste maatregel zal het risico van misbruik van identiteit dus aanzienlijk verkleinen.

In plaats van in detail de vorm en de inhoud van het verzoek te willen regelen, kunnen andere mechanismen worden ingesteld, bijvoorbeeld de mededeling van de nooddiensten aan de "Coördinatiecel" van de telefoonnummers die de nooddiensten gebruiken om de operatoren te bellen om hen bepaalde bewaarde gegevens te vragen.

Overigens is het essentieel dat het veiligheidsmechanisme dat werd ingevoerd tussen de nooddiensten die ter plaatse hulp bieden en de operatoren voor de

En effet, il n'est pas établi que des difficultés se posent à l'heure actuelle ou que la réglementation actuelle et les délégations au Roi contenues dans l'article 126/1 seraient insuffisantes. Par ailleurs, fixer la forme et le contenu des demandes présente également le risque d'imposer une charge administrative lourde et inefficace pour les opérateurs et les autorités concernées.

a) La demande émanant des services d'urgence:

Actuellement, les services d'urgence offrant de l'aide sur place ne disposent pas d'une ligne téléphonique directe vers les opérateurs pour réclamer les données d'identification de l'appelant que l'opérateur concerné par l'appel d'urgence ne leur a pas fourni comme il doit le faire conformément à l'article 107, § 2, de la loi. Ils doivent donc utiliser les mêmes canaux de communication que ceux utilisés par la population pour contacter l'opérateur, ce qui renforce l'importance que l'opérateur s'assure que l'appel émane bien des services d'urgence. Cependant, l'article 126/1 du projet de loi institue la "Cellule de coordination" au sein des opérateurs et fournisseurs, à laquelle les services d'urgence auront accès. C'est dans l'arrêté d'exécution de cet article qu'il faudra être attentif aux mécanismes de sécurité des demandes et transferts d'information, par exemple en obligeant les opérateurs à communiquer le numéro de la ligne téléphonique directe (non publique) de la Cellule de coordination aux services d'urgence offrant de l'aide sur place. Ceci sera possible dès lors que le texte de l'article 126/1, § 4, 3°, habilite le Roi à fixer "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" et que le paragraphe 1er de l'article 126/1 prévoit entre autres la communication à la Commission pour la protection de la vie privée et à l'IBPT des coordonnées de la "Cellule de coordination". Cette première mesure réduira donc sensiblement le risque d'usurpation d'identité.

A la place de vouloir régler en détail la forme et le contenu de la demande, d'autres mécanismes peuvent être mis en place, par exemple une communication des services d'urgence à la "Cellule de coordination" des numéros de téléphone que les services d'urgence utilisent pour appeler les opérateurs dans le but de leur demander certaines données conservées.

Par ailleurs, il est essentiel que le mécanisme de sécurité mis en place entre les services d'urgence offrant de l'aide sur place et les opérateurs pour le transfert des

overdracht van informatie, niet wordt vertraagd door taken en acties van deze nooddiensten, des te meer aangezien het leven van iemand ervan kan afhangen. Zware vormvoorschriften opgelegd bij koninklijk besluit moeten dus worden vermeden.

b) Het verzoek vanwege de "Cel Vermiste Personen" van de federale politie:

De mogelijkheid voor de "Cel Vermiste Personen" van de federale politie om haar verzoek te rechtstreeks aan de operator te richten, werd geschrapt. Deze dienst zal dus in alle gevallen zijn verzoek via een door de Koning aangeduide politiedienst moeten richten, bijvoorbeeld de dienst NTSU-CTIF. Bovendien is deze dienst welbekend zowel door deze cel aangezien deze cel zowel als de dienst NTSU-CTIF deel uitmaken van de federale gerechtelijke politie, als door de operatoren en kan deze dus onregelmatige of onrechtmatige verzoeken vermijden.

c) Het verzoek vanwege de Ombudsdienst voor telecommunicatie:

Ten eerste behandelde de Ombudsdienst over een termijn van circa 15 jaar reeds tienduizenden klachten betreffende kwaadwillige oproepen en werd deze nooit geconfronteerd met enigerlei problemen gerelateerd aan inbreuken tegen de privacy van de vermoedelijke dader.

Ten tweede geeft de Raad van State geen precieze indicatie over de specifieke garanties die zouden moeten worden gegeven door de Ombudsdienst waardoor het niet duidelijk is welke deze garanties zijn die momenteel zouden ontbreken.

Ten derde bepaalt artikel 43*bis*, § 3, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven onder andere wat volgt:

"De ombudsdienst heeft de volgende opdrachten: […]

7° van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische-communicatienetwerk of —dienst, het verzoek onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische-communicatienetwerken of —diensten die deze persoon hebben lastiggevallen, voorzover die gegevens beschikbaar zijn. De ombudsdienst willigt het verzoek in indien de volgende voorwaarden verenigd zijn:

a) de feiten lijken vast te staan;

informations ne ralentisse pas les tâches et actions de ces services d'urgence, d'autant plus que la vie d'une personne peut être en danger. Un formalisme lourd imposé par arrêté royal doit donc être évité.

b) La demande émanant de la "Cellule de disparition" de la police fédérale:

La possibilité pour le service "Cellule de disparition" de la police fédérale d'adresser sa demande directement à l'opérateur a été supprimée. Dès lors, ce service devra dans tous les cas formuler sa demande par l'intermédiaire d'un service de police désigné par le Roi, par exemple le NSU-CTIF. Or ce service est bien connu tant par cette cellule, dès lors que tant cette cellule que le NTSU-CTIF font partie de la police judiciaire fédérale, que par les opérateurs et peut donc éviter des demandes irrégulières ou abusives.

c) La demande émanant du Service de Médiation pour les télécommunications:

Premièrement, le Service de Médiation a déjà traité sur une délai de 15 ans des dizaines de milliers de plaintes concernant des appels malveillants et n'a jamais été confronté avec le moindre problème lié à une intrusion dans la vie privée de l'auteur présumé.

Deuxièmement, le Conseil d'État ne donne pas d'indication précise sur les garanties spécifiques qui devraient être mises par le Service de médiation, de sorte qu'il n'est pas clair quelles sont ces garanties qui feraient défaut à l'heure actuelle.

Troisièmement, l'article 43*bis*, § 3, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques prévoit entre autres ce qui suit:

"Le Service de Médiation est investi des missions suivantes: […]

7° examiner la demande de toute personne se prétendant victime d'une utilisation malveillante d'un réseau ou d'un service de communications électroniques visant à obtenir communication de l'identité et de l'adresse des utilisateurs de réseaux ou de services de communications électroniques l'ayant importunée, pour autant que ces données sont disponibles. Le service de médiation accède à la demande si les conditions suivantes sont réunies:

a) les faits semblent établis;

b) het verzoek heeft betrekking op precieze data en uren. “

Dankzij de controle uitgevoerd op basis van de hierboven vermelde criteria, probeert de Ombudsdienst de ongerechtvaardigde verzoeken of misbruiken te verwijderen.

Ten vierde luidt artikel 43*bis*, § 4, van diezelfde wet: “De ombudsdienst mag in het kader van een klacht die bij hem is ingediend, ter plaatse, kennis nemen van boeken, briefwisseling, processen-verbaal en in het algemeen van alle documenten en alle geschriften van de betrokken onderneming of ondernemingen die rechtstreeks betrekking hebben op het voorwerp van de klacht. [...] De aldus verkregen informatie behandelt de ombudsdienst vertrouwelijk, wanneer de verspreiding de onderneming op algemeen vlak zou kunnen schaden. “Dat principe van vertrouwelijkheid waaraan de Ombudsdienst is gehouden, vormt ook een garantie.

Ten vijfde weigert de Ombudsdienst eveneens aanvragen die niet worden ingediend via het daartoe bestemede formulier en die niet zijn ondertekend door de titularis van de betreffende aansluiting. De verificatie van het titularisschap gebeurt in samenwerking met de operator van de aansluiting waarop de vermoedelijke kwaadwillige oproepen hebben plaatsgevonden.

Er kan aldus geconcludeerd worden dat de bestaande procedure en werkwijze van de Ombudsdienst voldoende garanties bieden om de privacy van de oproepers veilig te stellen.

3. ***De creatie van een specifieke database om artikel 126 ten uitvoer te brengen***

De Raad van State stelt zich vragen bij de mogelijkheid om de data te bewaren krachtens artikel 126 in ontwerp in een databank die uitsluitend is bestemd voor de verzoeken van de overheden teneinde de risico's van niet-vernietiging van de betrokken gegevens zoveel mogelijk te beperken (punt 3.4.2.2.2.).

Deze piste kan niet worden gevolgd. Vanuit een technisch standpunt is het niet mogelijk door in een databank uitsluitend voor de data in kwestie te voorzien, om een betere naleving door de operator te garanderen van zijn verplichting tot vernietiging van de gegevens. Vanuit het standpunt van de controle op de vernietiging van de gegevens door het BIPT is het niet zo belangrijk dat de data die moeten bewaard worden krachtens artikel 126 afzonderlijk worden bewaard of samen met commerciële gegevens die mogen of moeten bewaard worden krachtens de artikelen 122 en 123 van de WEC. Teneinde het principe van de technologische neutraliteit na te leven,

b) la demande se rapporte à des dates et heures précises.”

Grâce au contrôle effectué sur base des critères repris ci-dessus, le Service de médiation essaie d'écarter les demandes injustifiés ou les abus.

Quatrièmement, l'article 43*bis*, § 4, de la même loi prévoit que “Le Service de Médiation peut, dans le cadre d'une plainte dont il est saisi, prendre connaissance, sur place, des livres, de la correspondance, des procès-verbaux et généralement de tous les documents et de toutes les écritures d'une ou des entreprises concernées ayant trait directement à l'objet de la plainte. […] L'information ainsi obtenue est traitée par le Service de Médiation comme confidentielle lorsque la divulgation pourrait nuire à l'entreprise sur un plan général.” Ce principe de confidentialité auquel le Service de médiation est tenu constitue également une garantie.

Cinquièmement, le Service de médiation refuse également les demandes qui ne sont pas introduites via le formulaire prévu à cet effet et qui ne sont pas signées par le titulaire de la ligne concernée. La vérification du titulaire se fait en collaboration avec l'opérateur de la ligne sur laquelle les appels malveillants présumés ont été effectués.

Il peut donc être conclu que la procédure et la méthode de travail existantes du Service de Médiation offrent des garanties suffisantes pour sauvegarder la vie privée des appelants.

3. ***La création d'une base de données spécifique pour mettre en œuvre l'article 126***

Le Conseil d'État s'interroge sur la possibilité de conserver les données en vertu de l”article 126 en projet dans une base de données exclusivement consacrée aux demandes des autorités afin de limiter de manière maximale les risques de non-destruction des données concernées (point 3.4.2.2.2.).

Cette piste ne peut être suivie. D'un point de vue technique, prévoir une base de données exclusivement consacrées aux données en question ne permet pas d'assurer un meilleur respect par l'opérateur de son obligation de destruction des données. D'un point de vue du contrôle de la destruction des données par l'IBPT, il importe peu que les données qui doivent être conservées en vertu de l'article 126 soient conservées séparément ou ensemble avec les données commerciales qui peuvent ou doivent être conservées en vertu des articles 122 et 123 de la loi du 3 juin 2005 relative aux communications électroniques. Afin de respecter le principe de neutralité

is het dus gepast om geen technologische keuzes op te leggen aan de operatoren en aanbieders wanneer deze verplichting geen daadwerkelijke meerwaarde heeft. Ook al worden de data die moeten worden bewaard conform artikel 126 bewaard in een database die specifiek voor deze data is bestemd, dat neemt niet weg dat de controle uitgevoerd door het BIPT ook betrekking moet hebben op de architectuur die de verschillende databanken onderbouwt, waaronder de databank bedoeld in artikel 126. Het zou ook gepast zijn om na te gaan dat de commerciële databank geen gegevens bevat die enkel door de autoriteiten mogen worden bewaard.

4. ***De controles en sancties in geval van niet-vernietiging van de data***

De Raad van State werpt op dat er in geen enkele strafrechtelijke incriminatie wordt voorzien inzake de niet-vernietiging van de gegevens na verstrijken van hun bewaringstermijn. Zo zou er ook geen enkele bepaling zijn die het BIPT verplicht om regelmatige en specifieke controles ter zake te verrichten (nr. 3.4.2.2.2.2.).

In tegenstelling tot wat de Raad van State stelt, voorziet het ontwerp van wet in de toevoeging van artikel 126 aan de lijst van artikelen vastgelegd in artikel 145 van diezelfde wet, artikelen waarvan de inbreuk een strafbaar feit vormt. De niet-naleving van artikel 126, het gebrek aan vernietiging van de data inbegrepen, zal dus strafrechtelijk worden bestraft.

Overigens houdt de verplichting van het BIPT tot het voeren van regelmatige controles op de vernietiging van de gegevens het risico in dat het BIPT niet langer de flexibiliteit heeft om gepaste controles uit te voeren op het juiste tijdstip en dus om deze controles doeltreffend te verrichten. Het BIPT moet immers zijn controles vastleggen niet alleen afhankelijk van het geheel van gevoelige data die worden behandeld door de operatoren (de metagegevens verwerkt door de operatoren voor commerciële doeleinden en de veiligheid van de inhoud van de communicatie die door hun netwerk passeert inbegrepen) maar ook naargelang van de concrete moeilijkheden die zich voordoen op het terrein.

technologique, il convient donc de ne pas imposer des choix technologiques aux opérateurs et fournisseurs, si cette obligation n'a pas de réelle plus-value. Même si les données qui doivent être conservées conformément à l'article 126 le sont dans une base de données dédiée à ces données, il n'empêche que le contrôle effectué par l'IBPT doit également porter sur l'architecture soutenant différentes bases de données, dont la base de données visée à l'article 126. Il conviendrait également de vérifier que la base des données commerciales ne contienne pas de données qui ne peuvent être conservées que pour les autorités.

4. ***Les contrôles et sanctions en cas de non-effacement des données***

Le Conseil d'État soulève qu'il n'est prévu aucune incrimination pénale en matière de non-destruction des données au terme de leur délai de conservation. De même, il n'y aurait aucune disposition imposant à l'IBPT d'effectuer des contrôles réguliers et spécifiques en la matière (n° 3.4.2.2.2.2.).

Contrairement à ce qui est avancé par le Conseil d'État, le projet de loi prévoit d'ajouter l'article 126 dans la liste d'articles prévue à l'article 145 de cette même loi, articles dont la violation constitue une infraction pénale. Le non-respect de l'article 126, en ce compris l'absence de destruction des données, sera donc sanctionné pénalement.

Par ailleurs, imposer à l'IBPT des contrôles réguliers concernant la destruction des données présente le risque d'enlever à l'IBPT la flexibilité pour effectuer des contrôles adéquats au bon moment et donc d'affecter l'efficacité de ces contrôles. En effet, l'IBPT doit fixer ses contrôles en fonction non seulement de l'ensemble des données sensibles traitées par les opérateurs (en ce compris des métadonnées traitées par les opérateurs à des fins commerciales et la sécurité du contenu des communication qui transite sur leur réseau) mais également en fonction des difficultés concrètes qui se présentent sur le terrain.

ARTIKELSGEWIJZE BESPREKING

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Artikel 1 verwijst naar de grondwettelijke bevoegdheidsverdeling.

HOOFDSTUK 2

Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2.

Dit artikel vervangt de definitie van het begrip "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 ontwerp 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, 4°.

Op dit ogenblik wordt de delegatie aan de Koning, waarvan sprake in artikel 125, § 2, ten uitvoer gelegd

COMMENTAIRES DES ARTICLES

CHAPITRE 1ER

Dispositions

Article 1er

L'article 1er renvoie à la répartition constitutionnelle des compétences.

CHAPITRE 2

Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 2.

Cet article remplace la définition de la notion 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

Le 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, 4°.

A l'heure actuelle, la délégation au Roi prévue à l'article 125, § 2, a été exécutée par l'arrêté royal du

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**

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 90*decies* 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 aan ten opzichte van de versie van artikel 126 die nietig is verklaard.

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. De wet van 8 december 1992 is de algemene wet die in elk geval van toepassing is inzake de bescherming van persoonsgegevens. Indien er een specifieke — lex specialis — bestaat, zoals de onderhavige wet, dan is deze van toepassing wat betreft de specifieke bepalingen ervan.

Daarom zijn de aanbieders en operatoren uitdrukkelijk verplicht alle bepalingen van de wet van

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**

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 90*decies* 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. La loi du 8 décembre 1992 est la loi générale qui s’applique en tout état de cause en matière de protection des données à caractère personnel. Si une loi spécifique — lex specialis — existe, telle que la présente loi, celle-ci s’applique pour ce qui concerne ses dispositions spécifiques.

Dès lors, les fournisseurs et opérateurs sont explicitement tenus de respecter l’ensemble des dispositions de

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 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.

3. **De ondernemingen die verplicht zijn tot gegevensbewaring**

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 operatoren die de onderliggende openbare elektronische-communicatie-netwerken aanbieden, alsook op de operatoren die een van deze diensten verstrekken.

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.

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.

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 90*decies* 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.

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 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. **Les entreprises tenues de conserver des données**

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 opérateurs fournissant des réseaux publics de communications électroniques sous-jacents ainsi qu'aux opérateurs fournissant un de ces services.

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.

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.

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 90*decies* 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 bewaartermijn van 12 maanden vast.

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

Het eerste lid van paragraaf 3 vermeldt "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.

Wat de gerechtelijke autoriteiten betreft, verwijst paragraaf 2 naar de artikelen 46*bis* en 88*bis* 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.

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 le délai de conservation de 12 mois.

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

L'alinéa 1 du paragraphe 3 se réfère 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.

Pour ce qui concerne les autorités judiciaires, le paragraphe 2 renvoie aux articles 46*bis* et 88*bis* 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.

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.

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) 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 en op het moment van de noodoproep overzenden 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

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.

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 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.

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. 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

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.

Het is niet gepast om de cel Vermiste Personen van de federale politie te verplichten een requisitoir van een procureur des Konings of van een onderzoeksrechter te vragen om gegevens te krijgen die door de operator of de aanbieder worden bewaard krachtens het onderhavige artikel, wanneer de onrustwekkende verdwijning niets te maken heeft met een strafbaar feit (vlucht, poging tot zelfmoord, enz.). Paragraaf twee bepaalt daarom dat de officier van gerechtelijke politie van de cel Vermiste Personen, via de door de Koning aangewezen politiedienst, bepaalde gegevens kan krijgen die worden bewaard door de operator of de aanbieder.

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.

Overigens bepaalde het voorontwerp van wet zoals voorgelegd aan de Raad van State dat “Het verzoek [van de Ombudsdienst voor de telecommunicatie] dient te worden gericht aan de betrokken aanbieder of operator binnen 8 dagen na het kwaadwillig gebruik van het netwerk of van de dienst.”

Deze beperking werd geschrapt aangezien ze de goede verwezenlijking van de opdrachten van de Ombudsdienst, die de volgende uitleg heeft aangebracht, in het gedrang kan brengen.

Gezien het feit dat dossiers ontvankelijk worden verklaard als wordt voldaan aan gecombineerde voorwaarden (te weten: de feiten lijken vast te staan; het verzoek heeft betrekking op precieze data en uren) hebben de meeste aanvragen betrekking tot een resem tijdstippen van kwaadwillige oproepen, vaak verspreid over een tijdsbestek welke de acht dagen overschrijdt. Om eventuele onterechte klachten en misbruiken te vermijden dient de Ombudsdienst bovendien elke aanvraag nauwkeurig te onderzoeken en te registreren in een databank, hetgeen eveneens een bepaalde impact heeft op het tijdsverloop. Tenslotte dient rekening te worden gehouden met de termijn die postcorrespondentie vereist, wanneer de aanvrager geen toegang heeft tot het aanvraagformulier op de website van de Ombudsdienst.

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 46*bis* en 88*bis* van het Wetboek van

données d’identification de l’appelant conservées sur base du présent article.

Il n’est pas approprié d’obliger la cellule de disparition de la police fédérale à solliciter un réquisitoire d’un procureur du Roi ou d’un juge d’instruction pour obtenir des données conservées par l’opérateur ou le fournisseur en vertu du présent article, lorsque la disparition inquiétante n’est pas le fait d’une infraction pénale (fugue, tentative de suicide, *etc.*). Le paragraphe deux prévoit dès lors que l’officier de police judiciaire de la cellule disparition peut obtenir certaines données conservées de l’opérateur ou du fournisseur par l’intermédiaire d’un service de police désigné par le Roi.

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.

Par ailleurs, l“avant-projet de loi tel que soumis au Conseil d”État prévoyait que “la demande [du service de médiation pour les télécommunications] est adressée au fournisseur ou à l’opérateur concerné dans les 8 jours suivant l’utilisation malveillante du réseau ou du service”.

Cette restriction a été supprimée, dès lors qu’elle est de nature à mettre en danger le bon accomplissement des mission du Service de médiation, qui a apporté les explications suivantes.

Étant donné que les dossiers sont déclarés recevables si des conditions combinées sont remplies (à savoir: les faits semblent établis; la demande se rapporte à des dates et heures précises), la plupart des demandes portent sur une série de dates et heures précises d’appels malveillants, souvent répartis sur une période supérieure à huit jours. Afin d’éviter d’éventuelles plaintes injustifiées et d’éventuels abus, le Service de médiation doit en outre étudier attentivement chaque demande et l’enregistrer dans une base de données, ce qui a également un certain impact sur les délais. Enfin, il convient de tenir compte des délais que nécessite la correspondance postale, lorsque le demandeur n’a pas accès au formulaire de demande sur le site Internet du Service de médiation.

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 46*bis* et 88*bis* du Code d’instruction

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.

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.

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.

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.

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.

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.

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.

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.

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. **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 existaient déjà dans la loi annulée. D'autre part, des mesures supplémentaires ont été rajoutées au paragraphe 4.

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.

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

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.

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 mettre 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 autorisée 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

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

8. **Terugbetaling van de kosten van de operatoren**

Artikel 126 voorziet niet in een compensatiemechanisme voor de kosten van de aanbieders en operatoren voor de 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.

Krachtens artikel 46*bis* en artikel 88*bis* 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.

De inlichtingen- en veiligheidsdiensten passen dezelfde tarieven toe overeenkomstig artikel 7 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.

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

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

8. **Remboursement des coûts des opérateurs**

L'article 126 ne prévoit pas de mécanisme de compensation des coûts des fournisseurs et opérateurs pour 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.

Par contre, des indemnités par réquisition sur la base de l'article 46*bis* et de l'article 88*bis* 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.

Les services de renseignement et de sécurité appliquent les mêmes tarifs conformément à l'article 7 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.

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

Art. 4

Paragraaf 1 van het nieuwe artikel 126/1 verplicht alle operatoren in de zin van de WEC en de aanbieders bedoeld in artikel 126, § 1, eerste lid, om een Coördinatiecel op te richten. Deze paragraaf 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.

Krachtens dit artikel 2 moet iedere operator van een elektronische-communicatienetwerk en iedere aanbieder van een elektronische-communicatiedienst een "Coördinatiecel Justitie" oprichten om te antwoorden op de requisitoirs die genomen zijn op basis van de artikelen 46*bis*, § 2, 88*bis*, § 2, en 90*quater*, § 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 dan ook niet beperkt tot de diensten van Justitie, wordt deze cel de Coördinatiecel.

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

Behoudens wat betreft de operatoren en aanbieders die geen van de diensten beoogd in artikel 126, § 1, verstrekken, moet elk lid van de Coördinatiecel 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.

Art. 4

Le paragraphe 1er du nouvel article 126/1 impose à tous les opérateurs au sens de la LCE et aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, de constituer une Cellule de coordination. Ce paragraphe 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.

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 coordination de la Justice "pour répondre aux réquisitoires pris sur base des articles 46*bis*, § 2, 88*bis*, § 2, et 90*quater*, § 2, du Code d'instruction criminelle. En 2010, la possibilité a été créée 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 limitent dès lors pas qu'aux services de la Justice, cette Cellule devient la Cellule de coordination.

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.

Sauf pour ce qui concerne les opérateurs et fournisseurs ne fournissant aucun des services visés à l'article 126, § 1er, 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.

De leden van de Coördinatiecel van de operatoren en aanbieders die geen dienst beoogd in artikel 126, § 1, verstrekken (telefoniediensten, ook via internet, internettoegangsdiensten en e-mail via het internet) hoeven niet te beschikken over een veiligheidsadvies. We denken hierbij aan de operatoren die bepaalde diensten verstrekken aan de ondernemingen (bijvoorbeeld huurlijnen) of aan andere operatoren.

Deze vrijstelling wordt verklaard door de volgende redenen. Aanvankelijk voorzag de tekst in een delegatie aan de Koning om versoepelingen in te voeren voor operatoren met een kleine omvang ten opzichte van dat veiligheidsadvies.

De Raad van State heeft zich vragen gesteld bij die mogelijkheid omdat het ingevoerde systeem niet mag leiden tot het ontnemen van bepaalde garanties die het voorontwerp geeft in termen van bescherming van een fundamenteel recht, namelijk dat van de bescherming van de persoonlijke levenssfeer, aan de personen van wie de data worden bewaard.

Het advies van de Raad van State werd gevolgd. Er wordt dan ook niet langer voorzien in een versoepeling voor de operatoren of aanbieders met een kleine omvang maar wel voor de aanbieders en de operatoren die geen van de diensten beoogd in artikel 126, § 1, van de wet verstrekken en wel om de volgende redenen.

Ten eerste verwijst de Raad van State naar de mogelijkheid voor de operatoren om een gemeenschappelijke “Coördinatiecel” op te richten als praktische oplossing voor de operatoren.

Tot op vandaag hebben de operatoren echter nog nooit een Coördinatiecel Justitie opgericht, wat een mogelijkheid is waarin artikel 2, § 2, van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie voorziet.

Ten tweede is het logisch om strengere regels toe te passen op de operatoren en aanbieders die data moeten bewaren voor de overheden (namelijk de operatoren en aanbieders beoogd in artikel 126, § 1) dan voor de operatoren en aanbieders die daar niet toe verplicht zijn.

Ten derde zijn het de operatoren en aanbieders die een van de diensten beoogd in artikel 126, § 1, eerste lid, bieden die bijna alle verzoeken vanwege de gerechtelijke overheden ontvangen.

Les membres de la Cellule de coordination des opérateurs et fournisseurs qui ne fournissent pas de services visés à l’article 126, § 1er (services de téléphonie, en ce compris par internet, d’accès à l’Internet et de courrier électronique par Internet), ne doivent pas disposer d’un avis de sécurité. On pense ici aux opérateurs qui fournissent certains services aux entreprises (par exemple des lignes louées) ou à d’autres opérateurs.

Cette exemption s’explique pour les raisons suivantes. Au départ, le texte prévoyait une délégation au Roi pour prévoir des assouplissements pour les opérateurs de petites tailles par rapport à cet avis de sécurité.

Le Conseil d’État s’est interrogé par rapport à cette possibilité, dès lors que le système mis en place ne peut aboutir au fait de priver les personnes dont les données sont conservées de certaines garanties que l’avant-projet leur donne en termes de protection d’un droit fondamental, celui du respect de la vie privée.

L’avis du Conseil d’État a été suivi, dès lorsqu’un assouplissement n’est plus prévu pour les opérateurs ou fournisseurs de petite taille mais bien pour les fournisseurs et les opérateurs qui n’offrent pas un des services visés à l’article 126, § 1er, de la loi et ce pour les raisons suivantes.

Premièrement, le Conseil d’État se réfère à la possibilité pour les opérateurs de créer une “Cellule de coordination” commune comme solution pratique pour les opérateurs.

Cependant, à ce jour, les opérateurs n’ont jamais constitué de Cellule de coordination de la Justice commune, qui est une possibilité prévue dans l’article 2, § 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.

Deuxièmement, il est logique d’appliquer des conditions plus sévères pour les opérateurs et fournisseurs devant conserver des données pour les autorités (soit les opérateurs et fournisseurs visés à l’article 126, § 1er) que pour des opérateurs et fournisseurs qui n’ont pas cette obligation.

Troisièmement, ce sont les opérateurs et fournisseurs qui offrent un des services visés à l’article 126, § 1er, alinéa 1er, qui reçoivent presque la totalité des demandes des autorités judiciaires.

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.

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. Artikel 126/1 bepaalt dat de aangestelde moet nagaan dat "enkel de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens". Zo moet de aangestelde de aanvragen van autoriteiten kunnen opsporen die duidelijk niet gemachtigd zijn om de gevraagde gegevens te krijgen. Het is mogelijk dat de aangestelde de hulp of samenwerking nodig heeft van de autoriteiten die bevoegd zijn om deze controle uit te voeren. Het spreekt daarentegen vanzelf dat het de taak is van de gerechtelijke autoriteiten en van de inlichtingen- en veiligheidsdiensten en niet die van de operator (inclusief de aangestelde) om zich te vergewissen van de geldigheid van het requisitoir dat gericht is aan de operator of om de naleving te controleren van het Wetboek van Strafvordering of van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Le 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.

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 préposé à la protection des données s'impose donc. L'article 126/1 prévoit que le préposé doit vérifier que "seules les autorités légalement autorisées aient accès aux données conservées". Ainsi, le préposé doit pouvoir détecter les demandes d'autorités qui, manifestement, ne sont pas autorisées à obtenir les données demandées. Le préposé pourrait avoir besoin de l'aide ou de la collaboration des autorités compétentes pour effectuer ce contrôle. Par contre, il va de soi qu'il revient aux autorités judiciaires et aux services de renseignement et de sécurité et non à l'opérateur (en ce compris le préposé) de s'assurer de la validité du réquisitoire adressé à l'opérateur ou de contrôler le respect du Code d'instruction criminelle ou de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

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.

Paragraaf 4 van het nieuwe artikel 126/1 voorziet in een reeks delegaties aan de Koning. Punt 2° moet 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 4° is geïnspireerd op paragraaf 2 van artikel 125, dat door de onderhavige wet wordt opgeheven.

Art. 5

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

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

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.

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.

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.

Le paragraphe 4 du nouvel article 126/1 prévoit une série de délégations au Roi. Le point 2° doit 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 4° s'inspire du paragraphe 2 de l'article 125 que la présente loi abroge.

Art. 5

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

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

Art. 6

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.

L'article 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.

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.

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.

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 550*bis*, § 1, van het Strafwetboek: externe hacking, met verzwarende omstandigheden in geval van bezit, onthulling, verspreiding of gebruik van de gegevens (§ § 3 en 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 550*bis*, § 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.

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

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

Wat dat betreft, voorziet artikel 39 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking

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.

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.

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.

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 550*bis*, § 1er, du Code pénal: le hacking externe, avec les circonstances aggravantes en cas de détention, divulgation, distribution ou usage des données (§ § 3 et 7).

Lorsqu'une personne est autorisée à accéder au système et outrepasse son pouvoir d'accès, il peut être renvoyé au hacking interne (article 550*bis*, § 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.

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

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

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

van persoonsgegevens, in een boete van 100 tot 100 000 EUR volgens de huidige van kracht zijnde wetgeving voor de verantwoordelijke 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.

HOOFDSTUK 3

Bepalingen tot wijziging van het Wetboek van strafvordering

Art. 8

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

Zoals reeds uitgelegd werd in het algemeen gedeelte van deze memorie van toelichting wordt een differentiatie ingevoerd voor wat betreft de toegang tot de gegevens voorzien in artikel 46*bis*. Voor lichtere misdrijven, die geen correctionele gevangenisstraf van één jaar of een zwaardere straf 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

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

amende pénale de 100 à 100 000 EUR selon la législation actuellement en vigueur pour tout responsable de traitement (ou 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.

CHAPITRE 3

Dispositions modifiant le Code d'instruction criminelle

Art. 8

Cet article ajoute un alinéa 4 au § 1er de l'article 46*bis* 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 46*bis*. Pour des infractions de moindre gravité, qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

Art. 9

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

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 90*decies* 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 46*bis* en 88*bis*, waar de materiële en procedurele voorwaarden vastgelegd zijn.

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 88*bis*, dat betrekking heeft op het opvragen van verkeers- en lokalisatiegegevens. Deze gegevens zijn immers meer privacygevoelig dan de identificatiegegevens bedoeld in artikel 46*bis*, in die zin dat ze, zoals het Europese Hof van Justitie in 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 wordt.

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 46*bis*, en anderzijds de verkeers- en lokalisatiegegevens bedoeld in artikel 88*bis*. Voor die laatste gelden sowieso al strengere voorwaarden en procedures.

Er worden wijzigingen aangebracht in artikel 88*bis* die voorzien in een differentiatie in termijnen voor wat betreft het opvragen van gegevens.

De wijzigingen die huidig ontwerp van wet in artikel 88*bis* 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.

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 90*decies* 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 46*bis* et 88*bis*, qui définissent les conditions matérielles et procédurales.

Afin de répondre aux préoccupations de la Cour, le gouvernement a décidé d'inclure des garanties et des conditions supplémentaires dans l'article 88*bis*, 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 46*bis* 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.

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 46*bis* et données de trafic et de localisation visées à l'article 88*bis*. Ces dernières font de toute manière déjà l'objet de conditions et de procédures plus strictes.

Des modifications sont apportées à l'article 88*bis* qui prévoient une différenciation en ce qui concerne les délais pour la demande de données.

Les modifications que le présent projet de loi apporte à l'article 88*bis* 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.

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 46*ter*), en het inwinnen van inlichtingen betreffende bankrekeningen (artikel 46*quater*).

Tegelijk wordt in dit eerste lid van § 1 de terminologie aangepast. Artikel 46*bis* spreekt immers over “de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst”, terwijl in artikel 88*bis* nog de oude terminologie wordt gehanteerd: “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”.

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 46*ter*) ainsi que la collecte de renseignements sur les comptes bancaires (article 46*quater*).

Par la même occasion, la terminologie est adaptée dans cet alinéa 1er du § 1er. Dans l’article 46*bis*, il est en effet question du “concours de l’opérateur d’un réseau de communication électronique ou d’un fournisseur d’un service de communication électronique” tandis que l’article 88*bis* 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° 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 46*bis* (op zich een mindere inbreuk op de privacy dan artikel 88*bis*): 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.

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 88*bis* 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.

In de nieuwe § 2 van artikel 88*bis* 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° Artikel 88*bis* is, samen met artikel 90*ter* 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

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 46*bis* (qui constitue en soi une infraction moindre à la vie privée que l'article 88*bis*): 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.

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 88*bis* 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.

Dans le nouveau § 2 de l'article 88*bis*, 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.

5° L'article 88*bis* est, avec l'article 90*ter* 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

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.

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. 40*bis*), de inkijkoperatie (art. 46*quinquies* en 89*ter*), de observatie (art. 47*sexies*), en de infiltratie (art. 47*octies*). Vandaar dat huidig artikel van het ontwerp van wet het ook in het geval van artikel 88*bis* 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 88*bis*, § 1, derde en vierde lid. De voorgestelde wijziging stelt de magistraat dus in staat om zijn requisitoir mondeling mee te delen aan de politiediensten. Deze politiediensten moeten er echter zorg voor dragen om een schriftelijk verzoek te sturen naar de operator, om fouten en fraude te voorkomen.

6° 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.

In § 1 werd al een proportionaliteitsvereiste ingevoegd door het toepassingsgebied van artikel 88*bis* 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.

De gegevens waarvan sprake in § 1 van artikel 88*bis* moeten in principe bewaard worden door de operatoren van elektronische communicatienetwerken en dienstenverstrekkers van elektronische communicatiediensten

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.

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 40*bis*), le contrôle visuel discret (articles 46*quinquies* et 89*ter*), l'observation (article 47*sexies*) et l'infiltration (article 47*octies*). C'est la raison pour laquelle le présent article du projet de loi permet, pour l'article 88*bis* 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 88*bis*, § 1er, alinéas 3 et 4. La modification proposée permet donc au magistrat de communiquer verbalement aux services de police son réquisitoire. Mais ces services de police prendront soin d'envoyer une demande écrite à l'opérateur, afin d'éviter les erreurs et les fraudes.

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.

Au § 1er, un principe de proportionnalité a déjà été inséré en limitant le champ d'application de l'article 88*bis* 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.

Les données dont il est question au § 1er de l'article 88*bis* doivent en principe être conservées par les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communication

op basis van artikel 126 van de wet betreffende de elektronische communicatie. Het gaat om de gegevens bedoeld in het tweede en derde lid van artikel 126, § 3, waarvoor de bewaartermijn op 12 maanden is bepaald vanaf de datum van de communicatie.

De bewaartermijn van 12 maanden kan, anders dan tot nu toe, door de onderzoeksrechter echter alleen volledig worden benut wanneer sprake is van terroristische misdrijven, dit wil zeggen de misdrijven bedoeld in Titel Iter van Boek II van het Strafwetboek.

Hij kan de gegevens opvragen voor een duur van 9 maanden wanneer het strafonderzoek betrekking heeft op een ander strafbaar feit bedoeld in artikel 90*ter*, § § 2 tot 4, of dat is gepleegd in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of dat een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kan 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 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 46*bis* en 88*bis*.

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 onderzoeksrechter.

électronique sur la base de l'article 126 de la loi relative aux communications électroniques. Il s'agit des données visées aux alinéas 2 et 3 de l'article 126, § 3, pour lesquelles le délai de conservation est fixé à 12 mois à partir 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 12 mois que lorsqu'il est question d'infractions terroristes, c'est-à-dire les infractions visées au Titre Iter du Livre II du Code pénal.

Il pourra requérir les données pour une durée de 9 mois lorsque la procédure pénale porte sur une autre infraction visée à l'article 90*ter*, § § 2 et 4, ou qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou qui est 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 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 46*bis* et 88*bis*.

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.

7° 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.

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 56*bis*), of de telefoontap (artikel 90*octies*). Zoals ook bij die maatregelen is voorzien, zal artikel 88*bis* 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.

In haar voormelde advies vraagt de Privacycommissie om journalisten op te nemen bij de beroepen die door § 3 worden beschermd. Zo'n toevoeging wordt niet nodig geacht omdat journalisten al het voordeel hebben van de bescherming die hun wordt geboden door de wet van 7 april 2005 tot bescherming van de journalistieke bronnen. De toegang tot de gegevens is maar mogelijk als de informatie als cruciaal wordt geacht voor de identificatie van en zoektocht naar de daders van misdrijven die de fysieke integriteit in gevaar brengen of om dergelijke feiten te voorkomen. Bovendien kan het journalistieke brongeheim maar worden opgeheven indien de gevraagde informatie op geen andere manier kan worden verkregen. De tussenkomst van de rechter waarborgt de naleving van deze vereisten (DOC 51-24/001, p. 13).

Overeenkomstig artikel 5 van de wet van 7 april 2005 mogen gegevens die betrekking hebben op de informatiebronnen van journalisten, niet het voorwerp uitmaken van enige opsporings- of onderzoeksmaatregel, tenzij die gegevens kunnen voorkomen dat misdrijven worden gepleegd die de fysieke integriteit van een of meer personen ernstig in het gedrang brengen, in de hierboven vermelde omstandigheden.

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.

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 56*bis*) ou de l'écoute téléphonique (article 90*octies*). À l'instar de ce qui a été prévu pour ces mesures, l'article 88*bis* 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.

Dans son avis précité, la Commission vie privée demande d'inclure les journalistes parmi les professions protégées par le § 3. Un tel ajout n'est pas jugé nécessaire car les journalistes bénéficient déjà de la protection qui leur est accordée par la loi du 7 avril 2005 relative à la protection des sources journalistes. L'accès aux données n'est possible que si l'information est jugée cruciale pour l'identification et la recherche des auteurs d'infractions mettant en danger l'intégrité physique ou pour éviter ce type d'infraction. En outre, le secret des sources journalistiques ne peut être levé que si l'information demandée ne peut être obtenue autrement. L'intervention du juge garantit le respect de ces exigences (DOC 51-24/001, p. 13)

En application de l'article 5 de la loi du 7 avril 2005, il ne pourra être procédé à aucune mesure d'information ou d'instruction concernant des données relatives aux sources d'information des journalistes, sauf si ces données sont susceptibles de prévenir la commission des infractions constituant une menace grave pour l'intégrité physique d'une ou de plusieurs personnes dans les conditions citées ci-avant.

In de voorbereiding van de wet van 7 april 2005 wordt duidelijk gezegd: “Het spreekt vanzelf dat de journalist zijn informatie op wettige wijze moet verkregen hebben. Dit houdt in dat een journalist die zijn informatie verkreeg door middel van een misdrijf strafrechtelijk vervolgd kan worden.” (DOC 51-24/001, p. 11)

Zoals bovendien eerder is gepreciseerd, weerspiegelt artikel 88*bis* hetgeen reeds bestaat in de artikelen 56*bis* en 90*octies*. Welnu, deze twee artikelen doelen enkel op advocaten of artsen.

8° Tot slot wordt in de oude § 2, die nu § 4 zal worden 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.

HOOFDSTUK IV

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

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

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

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

Les travaux préparatoires de la loi du 7 avril 2005 précisent que “Il va de soi que le journaliste doit avoir obtenu ses informations de manière licite. Un journaliste qui a obtenu ses informations en commettant une infraction sera donc passible de poursuites pénales.” (DOC 51-24/001, p. 11)

En outre, comme précisé précédemment, l’article 88*bis* reflète ce qui existe déjà dans les articles 56*bis* et 90*octies*. Or, ces deux articles visent uniquement l’avocat ou le médecin.

8° Enfin, dans l’ancien § 2 (qui deviendra le § 4) qui impose le concours des opérateurs et des fournisseurs de services, la terminologie sera également adaptée comme détaillé au point 1°.

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.

CHAPITRE IV

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

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° 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.

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

van de oorsprong of de bestemming van de elektronische communicatie, vallen onder deze bescherming die onontbeerlijk is ten aanzien van de persoonlijke levenssfeer.

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.

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:

ou de la destination de communications électroniques, feront l'objet de cette protection indispensable au respect de la vie privée.

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.

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:

— 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 potentiële 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 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°.”.

4° Het derde lid van § 1 met betrekking tot het aanwenden van specifieke methodes ten opzichte van advocaten, artsen en journalisten, dat voorziet in een bijzondere beschermingsprocedure voor deze categorieën van personen, wordt § 5 van artikel 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 op de controle door de Commissie.

6° De toevoeging van een nieuwe § 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.

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

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

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

— 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.

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° 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° 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 au contrôle de la Commission.

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 (modification art. 18/8 loi Renseignement)

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.

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

het diensthoofd en pas ten uitvoer kan gelegd worden na kennisgeving aan de BIM-Commissie (zie MvT bij artikel 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 huidig ontwerp 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”.

2° De wijziging in § 1, tweede lid, is louter terminologisch. Er kan verwezen worden naar de toelichting onder punt 1°.

3° Net als voor de toegang tot de gegevens in het kader van strafrechtelijke vervolging voert het wetsontwerp een differentiatie in van de termijnen met betrekking tot de toegang tot de gegevens door de inlichtingendiensten. Er wordt voorzien in twee systemen naargelang van het soort van dreiging.

Wanneer de potentiële dreiging uitgaat van activiteiten gelieerd aan criminele organisaties of schadelijke sektarische organisaties, mogen de gegevens slechts voor een periode van 6 maanden opgevraagd worden. In die 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

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).

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.

Les modifications apportées à l’article 18/8 par le présent 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° La modification apportée au § 1er , alinéa 2, est purement terminologique. Il peut être renvoyé aux explications reprises au point 1°.

3° Comme pour l’accès aux données dans le cadre des poursuites pénales, le projet de loi introduit une différenciation des délais concernant l’accès aux données par les services de renseignement. Deux régimes sont prévus en fonction du type de menace.

Lorsque la menace potentielle émane d’activités en rapport avec les organisations criminelles ou les organisations sectaires nuisibles, les données ne peuvent être demandées que pour une période de 6 mois. Dans cette 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

het onderzoek naar een aantal dreigingen wordt teruggebracht van 12 maanden naar 6 maanden.

Wanneer de potentiële dreiging uitgaat van activiteiten gelieerd aan terrorisme of extremisme, mogen de gegevens voor een periode van 12 maanden opgevraagd worden.

Voor de andere soorten van dreiging die onder de opdrachten van de inlichtingendiensten vallen, wordt een tussenliggende termijn van 9 maanden vastgesteld. Het gaat bijvoorbeeld over dreigingen die verband houden met spionage, inmenging of verspreiding van massavernietigingswapens.

Het voorontwerp van wet, zoals voorgelegd aan de Raad van State, deelde de "inmenging" in onder de dreigingsvormen, opgevolgd door de inlichtingendiensten, voor dewelke de duur van toegang tot de gegevens het kortst is (zes maanden). Er werd inmiddels beslist om dit aspect te wijzigen. Inmenging is een activiteit die wordt opgevolgd door de inlichtingendiensten. Ze wordt gedefinieerd als "de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden" (organieke wet, artikel 8, 1°, g). Deze inmenging van bijvoorbeeld buitenlandse Staten in de Belgische binnenlandse aangelegenheden kan een belangrijke weerslag hebben op bepaalde bevolkingsgroepen, waaronder deze die gelinkt zijn aan de uitoefening van een eredienst. In bepaalde gevallen is er een band tussen de contra-inmenging en de strijd tegen het radicalisme, die een prioriteit vormt.

4° De huidige § 2 met betrekking tot de hoogdringendheidsprocedure wordt vernummerd tot § 4.

De minister van Justitie,

Koen GEENS

De minister van Digitale Agenda, Telecom en Post,

Alexander DE CROO

De minister van Defensie,

Steven VANDEPUT

disponibles pour l'enquête relative à un certain nombre de menaces est réduite de 12 mois à 6 mois.

Lorsque la menace potentielle émane d'activités en rapport avec le terrorisme ou l'extrémisme, les données peuvent être demandées pour une période de 12 mois.

Pour les autres types de menace entrant dans les missions des services de renseignement, un délai intermédiaire de 9 mois est prévu. Cela concerne par exemple les menaces liées à l'espionnage, à l'ingérence ou à la prolifération d'armes de destruction massive.

L'avant-projet de loi soumis au Conseil d'État classait l' "ingérence" parmi les types de menaces suivies par les services de renseignement pour lesquels la durée d'accès aux données est la plus courte (six mois). Il a été décidé entretemps de modifier cet aspect. L'ingérence est une des activités suivies par les services de renseignement. Elle est définie comme "la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins" (loi organique, article 8, 1°, g). Cette immixtion par exemple d'États étrangers dans les affaires intérieures belges peut avoir un impact important sur certaines populations, y compris pour ce qui concerne l'exercice du culte. Il y a dans certains cas un lien entre la contre-ingérence et la lutte contre le radicalisme qui est une priorité.

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

Le ministre de la Justice,

Koen GEENS

Le ministre de l'Agenda numérique, des Télécom et de la Poste,

Alexander DE CROO

Le ministre de la Défense,

Steven VANDEPUT

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

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

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid zoals bepaald in artikel 74 van de Grondwet.

HOOFDSTUK 2

Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie

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:

1° de bepaling onder 11° wordt vervangen als volgt:

"11° "operator": een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9;";

2° het artikel wordt aangevuld met een bepaling onder 74° luidende als volgt:

"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. ".

Art. 3

Artikel 125, § 2, gewijzigd bij de wetten van 10 juli 2012 en 27 maart 2014, van dezelfde wet wordt opgeheven.

Art. 4

Artikel 126 van dezelfde wet wordt vervangen als volgt:

"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 operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

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

CHAPITRE 1ER

Dispositions générales

Article 1er

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

CHAPITRE 2

Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 2

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° le 11° est remplacé par ce qui suit:

"11° "opérateur": toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;";

2° l'article est complété par un 74° rédigé comme suit:

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

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

L'article 126 de la même loi est remplacé par ce qui suit:

"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 opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces

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.

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

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:

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

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

§ 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:

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 46*bis* en 88*bis* van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen.

2° De inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren 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 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

services, 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.

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

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

§ 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° 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 46*bis* et 88*bis* du Code d'instruction criminelle et dans les conditions fixées par ces articles.

2° Les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil 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.

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

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 43*bis*, § 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 gericht aan de betrokken aanbieder of operator binnen 8 dagen na het kwaadwillig gebruik van het netwerk of van de dienst.

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.

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.

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

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, maar exclusief de gegevens waarin het vierde lid voorziet, worden bewaard gedurende 12 maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende 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 3 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:

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 43*bis*, § 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 8 jours suivant l'utilisation malveillante du réseau ou du service.

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.

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. 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 et 3, 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.

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 à l'exclusion des données prévues à l'alinéa 4, sont conservées pendant 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, sont conservées pendant 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 3 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° 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 126/1, § 1;

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

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;

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;

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. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.

§ 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.

Die statistieken omvatten met name:

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens 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.

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;

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

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° 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° 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. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 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.

Ces statistiques comprennent notamment:

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

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

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

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 90*decies* 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 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.

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.

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

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.

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.

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:

§ 1er. 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 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.

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.

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

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° 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.

De Koning kan, bij een in Ministerraad overlegd besluit, beslissen dat bepaalde categorieën van operatoren of aanbieders niet onderworpen zijn aan de voorwaarden die worden beoogd in het derde lid of kan voor deze categorieën minder strikte voorwaarden vastleggen.

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.

De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.

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 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.

§ 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.

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.

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.

§ 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. De Koning mag evenwel, bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de categorieën bepalen van aanbieders of operatoren waarvoor deze onverenigbaarheid niet van toepassing is.

Bij de uitvoering van zijn opdrachten handelt de aangestelde voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid, en heeft hij toegang tot alle

Le Roi peut, par arrêté délibéré en Conseil des ministres, décider que certaines catégories d'opérateurs ou fournisseurs ne sont pas soumises aux conditions visées au troisième alinéa ou fixer pour ces catégories des conditions moins strictes.

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.

Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.

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 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. 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.

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.

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. 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. Le Roi peut toutefois, par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée, déterminer les catégories de fournisseurs ou d'opérateurs pour lesquels cette incompatibilité n'est pas applicable.

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

persoonsgegevens die worden bezorgd aan de autoriteiten, alsook tot alle relevante lokalen van de aanbieder of de operator.

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.

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

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

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

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

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

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.

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.

§ 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:

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

transmises aux autorités ainsi qu'à tous les locaux pertinents du fournisseur ou de l'opérateur.

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.

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

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

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

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

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

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.

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

2° paragraaf zes wordt opgeheven.

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:

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

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

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

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

1° 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;

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.".

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° le paragraphe 6 est abrogé.

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

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

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

"§ 3*ter*. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126;

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

Art. 8

In artikel 46*bis*, § 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:

"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."

Art. 9

In artikel 88*bis* 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:

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

"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:

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

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

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

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

"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."

CHAPITRE 3

Dispositions modifiant le Code d'instruction criminelle

Art. 8

A l'article 46*bis*, § 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:

"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

A l'article 88*bis* 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° Au § 1er, l'alinéa 1er est remplacé comme suit:

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

"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:

"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."

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

"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."

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

"§ 2. Wat betreft de toepassing van de maatregel bedoeld in § 1 op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

— Voor een strafbaar feit bedoeld in Titel Iter van Boek II van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van 12 maanden voorafgaand aan zijn bevelschrift.

— Voor andere strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, of die gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* 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 vorderen voor een periode van 9 maanden voorafgaand aan het bevelschrift;

— Voor andere strafbare feiten niet bedoeld in de vorige twee onderdelen, 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."

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 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."

4° § 1er, alinéa 4, est remplacé par:

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

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

"§ 2. Pour ce qui concerne l'application de la mesure visée au § 1er aux données de trafic ou de localisation conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:

— Pour une infraction visée au Titre Iter du Livre II du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de 12 mois préalable à l'ordonnance.

— Pour les autres infractions visées à l'article 90*ter*, §§ 2 à 4, ou qui sont commises dans le cadre d'une organisation criminelle visée à l'article 324*bis* 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 pour une période de 9 mois préalable à l'ordonnance.

— Pour d'autres infractions non visées par les deux points précédents, 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."

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 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° 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 90*decies* 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:

“De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die zij leveren.”

3° Er wordt een vierde lid ingevoegd, luidend als volgt:

“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.”

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:

1° Er wordt een § 2 ingevoegd, luidend als volgt:

“§ 2. De beslissing van het diensthoofd vermeldt:

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 90*decies* 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:

“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° Un quatrième alinéa est inséré, libellé comme suit:

“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

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° Un § 2 est inséré, libellé comme suit:

“§ 2. La décision du dirigeant du service mentionne:

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 Commissie;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode 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 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."

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° tot 3°, 5° en 7°.".

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

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

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

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

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

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

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

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."

Art. 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 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."

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

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

"§ 2. Wat betreft de toepassing van de methode bedoeld in § 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

1°) 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 slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing.

2°) Voor een potentiële bedreiging zoals bedoeld in artikel 18/1, andere dan deze bedoeld in 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing.

3° Voor een potentiële bedreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van 12 maanden voorafgaand aan zijn beslissing.

4° § 2 wordt vernummerd tot § 4.

avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la Commission de sa décision."

Art. 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:

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 adressées ou ont été adressées;

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

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

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

"§ 2. Pour ce qui concerne l'application de la méthode visée au § 1er aux données conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:

1°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée à l' ingérence, aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut requérir les données que pour une période de six mois préalable à la décision.

2°) Pour une menace potentielle autre que celles visées sous 1° et 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision.

3°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de 12 mois préalable à la décision.

4° Le § 2 est renuméroté en § 4.

ADVIES VAN DE RAAD VAN STATE NR. 58.449/4 VAN 7 DECEMBER 2015

Op 6 november 2015 is de Raad van State, afdeling Wetgeving, door de minister van Justitie verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet "betreffende de bewaring van gegevens in de elektronische-communicatiesector".

Het voorontwerp is door de vierde kamer onderzocht op 7 december 2015. De kamer was samengesteld uit Pierre Liénardy, kamervoorzitter, Martine Baguet en Bernard Blero, staatsraden, Sébastien Van Drooghenbroeck en Jacques Englebert, assessoren, en Colette Gigot, griffier.

Het verslag is uitgebracht door Anne Vagman, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre Liénardy en Martine Baguet.

Het advies, waarvan de tekst hierna volgt, is gegeven op 7 december 2015.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de gecoördineerde wetten op de Raad van State, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat deze drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

ALGEMENE OPMERKINGEN

I. STREKKING VAN HET VOORONTWERP, EUROPEES RECHT EN EUROPESE RECHTSPRAAK, INTERNE RECHTSPRAAK

1. Het Hof van Justitie van de Europese Unie heeft bij een arrest van de Grote kamer van 8 april 2014, gewezen naar aanleiding van de prejudiciële vragen van de High Court van Ierland en het Verfassungsgerichtshof van Oostenrijk (HvJ, C-293/12, Digital Rights Ireland Ltd, en C-594/12, Kärntner Landesregierung e.a.), 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" (hierna richtlijn 2006/24/EG genoemd) ongeldig verklaard.

De motivering en de beslissing van dat arrest luiden als volgt:

AVIS DU CONSEIL D'ÉTAT N° 58.449/4 DU 7 DÉCEMBRE 2015

Le 6 novembre 2015, le Conseil d'État, section de législation, a été invité par le ministre de la Justice à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi "relative à la conservation des données dans le secteur des communications électroniques".

L'avant-projet a été examiné par la quatrième chambre le 7 décembre 2015. La chambre était composée de Pierre Liénardy, président de chambre, Martine Baguet et Bernard Blero, conseillers d'État, Sébastien Van Drooghenbroeck et Jacques Englebert, assesseurs, et Colette Gigot, greffier.

Le rapport a été présenté par Anne Vagman, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Liénardy et Martine Baguet.

L'avis, dont le texte suit, a été donné le 7 décembre 2015.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois coordonnées sur le Conseil d'État, la section de législation limite son examen au fondement juridique de l'avant-projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

OBSERVATIONS GÉNÉRALES

I. PORTÉE DE L'AVANT-PROJET, DROIT ET JURISPRUDENCE EUROPÉENS, JURISPRUDENCE INTERNE

1. Par un arrêt du 8 avril 2014, rendu en grande chambre en réponse aux questions préjudicielles de la Haute Cour d'Irlande et de la Cour constitutionnelle d'Autriche (C.J.U.E., C-293/12, Digital Rights Ireland Ltd et C-594/12, Kärntner Landesregierung e.a.), la Cour de justice de l'Union européenne a invalidé la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 "sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la directive 2002/58/CE" (ci-après, la directive 2006/24/CE).

Cet arrêt est motivé et décide comme suit:

"Bestaan van inmenging in de in de artikelen 7 en 8 van het Handvest neergelegde rechten

(…)

34. (…) de door de artikelen 3 en 6 van richtlijn 2006/24 aan aanbieders van openbaar beschikbare elektronischecommunicatiediensten of een openbaar communicatienetwerk opgelegde verplichting om gegevens betreffende het privéleven van een persoon en zijn communicaties, zoals die welke zijn bedoeld in artikel 5 van deze richtlijn, gedurende een bepaalde tijd te bewaren, [vormt] op zich een inmenging (…) in de door artikel 7 van het Handvest gewaarborgde rechten.

35. Bovendien vormt de toegang van de bevoegde nationale autoriteiten tot de gegevens een aanvullende inmenging in dat fundamentele recht (zie met betrekking tot artikel 8 EVRM, arresten EHRM, Leander/Zweden, 26 maart 1987, reeks A nr. 116, § 48; Rotaru/Roemenië [Grote kamer], nr. 28341/95, § 46, CEDH 2000-V, en Weber en Saravia/Duitsland (dec.), nr. 54934/00, § 79, CEDH 2006-XI). De artikelen 4 en 8 van richtlijn 2006/24, die de toegang van de bevoegde nationale autoriteiten tot de gegevens regelen, vormen dus eveneens een inmenging in de door artikel 7 van het Handvest gewaarborgde rechten.

36. Richtlijn 2006/24 vormt ook een inmenging in het door artikel 8 van het Handvest gewaarborgde fundamentele recht op bescherming van persoonsgegevens, aangezien zij voorziet in de verwerking van persoonsgegevens.

37. Vastgesteld moet worden dat richtlijn 2006/24 een zeer ruime en bijzonder zware inmenging vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele rechten, zoals de advocaat-generaal met name in de punten 77 en 80 van zijn conclusie heeft opgemerkt. Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt.

Rechtvaardiging van de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten

38. Volgens artikel 52, lid 1, van het Handvest moeten beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en kunnen, met inachtneming van het evenredigheidsbeginsel, alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.

39. Wat de wezenlijke inhoud van het fundamentele recht op eerbiediging van het privéleven en de andere door artikel 7 van het Handvest erkende rechten betreft, moet worden

"Sur l'existence d'une ingérence dans les droits consacrés par les articles 7 et 8 de la Charte

[...]

34. [...] l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.

35. En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n° 116, § 48; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte.

36. De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel.

37. Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.

Sur la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte

38. Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

39. En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte, il convient de constater

vastgesteld dat de door richtlijn 2006/24 voorgeschreven bewaring van gegevens weliswaar een bijzonder zware inmenging in deze rechten vormt, maar niet raakt aan de inhoud ervan, aangezien deze richtlijn, zoals blijkt uit artikel 1, lid 2, ervan, niet de mogelijkheid biedt om kennis te nemen van de inhoud zelf van de elektronische communicaties.

40. Deze bewaring van gegevens doet evenmin afbreuk aan de wezenlijke inhoud van het door artikel 8 van het Handvest erkende fundamentele recht op bescherming van persoonsgegevens, aangezien richtlijn 2006/24 in artikel 7 ervan een regel inzake gegevensbescherming en -beveiliging bevat op grond waarvan de aanbieders van openbaar beschikbare elektronischecommunicatiediensten of van een publiek communicatienetwerk, onverminderd de bepalingen die zijn goedgekeurd ingevolge de richtlijnen 95/46 en 2002/58, bepaalde beginselen van gegevensbescherming en -beveiliging moeten respecteren. Volgens deze beginselen moeten de lidstaten ervoor zorgen dat passende technische en organisatorische maatregelen worden genomen om te vermijden dat de gegevens per ongeluk of onrechtmatig worden vernietigd dan wel per ongeluk verloren geraken of worden gewijzigd.

41. Met betrekking tot de vraag of deze inmenging voldoet aan een doel van algemeen belang, zij opgemerkt dat richtlijn 2006/24 weliswaar strekt tot harmonisatie van de bepalingen van de lidstaten betreffende de verplichtingen van bovengenoemde aanbieders inzake de bewaring van bepaalde gegevens die door hen worden gegenereerd of verwerkt, maar dat het materiële doel van deze richtlijn, zoals blijkt uit artikel 1, lid 1, ervan, erin bestaat te garanderen dat die gegevens beschikbaar zijn met het oog op het onderzoek, de opsporing en de vervolging van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten. Deze richtlijn heeft dus materieel tot doel om tot de bestrijding van ernstige criminaliteit en aldus uiteindelijk tot de openbare veiligheid bij te dragen.

42. Volgens de rechtspraak van het Hof vormt de bestrijding van terrorisme ter handhaving van de internationale vrede en veiligheid een doel van algemeen belang van de Unie (zie in die zin arresten Kadi en Al Barakaat International Foundation/Raad en Commissie, C-402/05 P en C-415/05 P, EU:C:2008:461, punt 363, en Al-Aqsa/Raad, C-539/10 P en C-550/10 P, EU:C:2012:711, punt 130). Hetzelfde geldt voor de bestrijding van ernstige criminaliteit ter waarborging van de openbare veiligheid (zie in die zin arrest Tsakouridis, C-145/09, EU:C:2010:708, punten 46 en 47). In dit verband zij voorts opgemerkt dat artikel 6 van het Handvest bepaalt dat eenieder niet alleen recht heeft op vrijheid, maar ook op veiligheid.

43. Dienaangaande blijkt uit punt 7 van de considerans van richtlijn 2006/24 dat de Raad justitie en binnenlandse zaken van 19 december 2002 wegens de opmerkelijke toename van de mogelijkheden van elektronische communicatie heeft geoordeeld dat gegevens betreffende het gebruik daarvan van bijzonder belang zijn en dus een waardevol instrument vormen bij het voorkomen van strafbare feiten en het bestrijden van criminaliteit, met name van de georganiseerde misdaad.

que, même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1er, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

40. Cette conservation des données n'est pas non plus de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, sans préjudice des dispositions adoptées en application des directives 95/46 et 2002/58, certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, principes selon lesquels les États membres veillent à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

41. Quant à la question de savoir si ladite ingérence répond à un objectif d'intérêt général, il convient de relever que, si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

42. Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU:C:2008:461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU:C:2012:711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU:C:2010:708, points46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté.

43. À cet égard, il ressort du considérant 7 de la directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil "Justice et affaires intérieures" du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.

44. De door richtlijn 2006/24 voorgeschreven bewaring van gegevens, die de bevoegde nationale autoriteiten de mogelijkheid moet bieden om deze eventueel te raadplegen, beantwoordt dus daadwerkelijk aan een doel van algemeen belang.

45. In deze omstandigheden moet worden nagegaan of de vastgestelde inmenging evenredig is.

46. Dienaangaande zij eraan herinnerd dat het evenredigheidsbeginsel volgens vaste rechtspraak van het Hof vereist dat handelingen van de instellingen van de Unie geschikt zijn om de door de betrokken regeling nagestreefde legitieme doelstellingen te verwezenlijken en niet verder gaan dan wat daarvoor geschikt en noodzakelijk is (zie in die zin arresten Afton Chemical, C-343/09, EU:C:2010:419, punt 45; Volker und Markus Schecke en Eifert, EU:C:2010:662, punt 74; Nelson e.a., C-581/10 en C-629/10, EU:C:2012:657, punt 71; Sky Österreich, C-283/11, EU:C:2013:28, punt 50, en Schaible, C-101/12, EU:C:2013:661, punt 29).

47. Wat het rechterlijk toezicht op de naleving van deze voorwaarden betreft, zij opgemerkt dat wanneer sprake is van een inmenging in fundamentele rechten, de omvang van de beoordelingsbevoegdheid van de wetgever van de Unie beperkt kan zijn. Dit hangt af van een aantal factoren, waaronder met name het betrokken domein, de aard van het door het Handvest gewaarborgde recht dat aan de orde is, alsook de aard, de ernst en het doel van de inmenging (zie naar analogie met betrekking tot artikel 8 EVRM, arrest EHRM, S en Marper/Verenigd Koninkrijk [Grote kamer], nrs. 30562/04 en 30566/04, § 102, CEDH 2008-V).

48. Gelet op de belangrijke rol die de bescherming van persoonsgegevens speelt in het licht van het fundamentele recht op bescherming van het privéleven, alsook op de omvang en de ernst van de door richtlijn 2006/24 veroorzaakte inmenging in dit recht is de beoordelingsbevoegdheid van de Uniewetgever in casu beperkt, zodat een strikt toezicht moet worden uitgeoefend.

49. Met betrekking tot de vraag of het door richtlijn 2006/24 nagestreefde doel kan worden verwezenlijkt door de bewaring van de gegevens, moet worden vastgesteld dat de gegevens die op grond van deze richtlijn moeten worden bewaard, gelet op het groeiende belang van elektronischecommunicatiemiddelen de nationale strafvervolgingsautoriteiten extra mogelijkheden bieden om ernstige gevallen van criminaliteit op te helderen en in die zin dus een waardevol instrument vormen bij strafonderzoeken. De bewaring van dergelijke gegevens is derhalve geschikt voor de verwezenlijking van het door deze richtlijn nagestreefde doel.

50. Aan deze beoordeling wordt niet afgedaan door de omstandigheid dat er verschillende vormen van elektronische communicatie bestaan die niet binnen de werkingssfeer van richtlijn 2006/24 vallen of die anonieme communicatie mogelijk maken, zoals met name Tschohl en Seitlinger alsook de Portugese regering in hun bij het Hof ingediende schriftelijke opmerkingen hebben aangevoerd. Dit heeft weliswaar tot gevolg dat de bewaring van gegevens niet volstrekt geschikt

44. Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24, répond effectivement à un objectif d'intérêt général.

45. Dans ces conditions, il y a lieu de vérifier la proportionnalité de l'ingérence constatée.

46. À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (voir, en ce sens, arrêts Afton Chemical, C-343/09, EU:C:2010:419, point 45; Volker und Markus Schecke et Eifert, EU:C:2010:662, point 74; Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, point 71; Sky Österreich, C-283/11, EU:C:2013:28, point 50, ainsi que Schaible, C-101/12, EU:C:2013:661, point 29).

47. En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt Cour EDH, S et Marper c. Royaume-Uni [GC], n^{os} 30562/04 et 30566/04, § 102, CEDH 2008-V).

48. En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

49. En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

50. Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure

is om het nagestreefde doel te bereiken, maar dat betekent nog niet dat deze maatregel daarvoor ongeschikt is, zoals de advocaat-generaal in punt 137 van zijn conclusie heeft opgemerkt.

51. Wat de noodzaak van de door richtlijn 2006/24 voorgeschreven bewaring van gegevens betreft, zij vastgesteld dat de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd.

52. Wat het recht op eerbiediging van het privéleven betreft, zij opgemerkt dat de bescherming van dit fundamentele recht volgens vaste rechtspraak van het Hof hoe dan ook vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (arrest IPI, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

53. Dienaangaande zij eraan herinnerd dat de bescherming van persoonsgegevens, die uitdrukkelijk wordt voorgeschreven door artikel 8, lid 1, van het Handvest, van bijzonder belang is voor het in artikel 7 van dit Handvest verankerde recht op eerbiediging van het privéleven.

54. De betrokken Unieregeling moet dus duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens (zie naar analogie met betrekking tot artikel 8 EVRM, arresten EHRM, Liberty e.a./Verenigd Koninkrijk, nr. 58243/00, § 62 en 63, van 1 juli 2008; Rotaru/Roemenië, reeds aangehaald, § 57-59, en S en Marper/Verenigd Koninkrijk, reeds aangehaald, § 99).

55. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens, zoals is bepaald in richtlijn 2006/24, automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (zie naar analogie met betrekking tot artikel 8 EHRM, arresten EHRM, S en Marper/Verenigd Koninkrijk, reeds aangehaald, § 103, en M. K./Frankrijk, nr. 19522/09, § 35, van 18 april 2013).

56. Met betrekking tot de vraag of de inmenging die richtlijn 2006/24 meebrengt, beperkt is tot het strikt noodzakelijke, zij opgemerkt dat artikel 3 van deze richtlijn, gelezen in samenhang met artikel 5, lid 1, ervan, voorschrijft om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren. Deze richtlijn strekt zich dus uit tot alle wijdverspreide elektronischecommunicatiemiddelen, die een steeds

de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

51. En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

52. S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

53. À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci.

54. Ainsi, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, n° 58243/00, § 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

55. La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, S et Marper c. Royaume-Uni, précité, § 103, ainsi que M. K. c. France, n° 19522/09, § 35, du 18 avril 2013).

56. Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de

belangrijker plaats innemen in het dagelijkse leven van de mensen. Bovendien ziet deze richtlijn ingevolge artikel 3 ervan op alle abonnees en geregistreerde gebruikers. Zij leidt dus tot inmenging in de fundamentele rechten van bijna de gehele Europese bevolking.

57. Dienaangaande zij in de eerste plaats vastgesteld dat richtlijn 2006/24 algemeen van toepassing is op alle personen, alle elektronischecommunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden.

58. Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit. Bovendien bevat de richtlijn geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het zakengeheim vallen.

59. Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.

60. In de tweede plaats bevat richtlijn 2006/24 niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. Integendeel, richtlijn 2006/24 verwijst in artikel 1, lid 1, ervan enkel op algemene wijze naar ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

61. Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Artikel 4 van deze richtlijn, dat de toegang van deze autoriteiten tot de bewaarde gegevens regelt, bepaalt niet uitdrukkelijk dat deze toegang en het latere gebruik van

communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

57. À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

58. En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59. D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

60. En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

61. En outre, quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation

de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen, maar bepaalt enkel dat elke lidstaat de procedure en de te vervullen voorwaarden vaststelt voor toegang tot de bewaarde gegevens overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid.

62. In het bijzonder bevat richtlijn 2006/24 geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel. Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Aan de lidstaten is evenmin enige specifieke verplichting opgelegd om dergelijke beperkingen vast te stellen.

63. Wat in de derde plaats de termijn betreft gedurende welke de gegevens worden bewaard, bepaalt artikel 6 van richtlijn 2006/24 dat deze gedurende ten minste zes maanden moeten worden bewaard, zonder dat enig onderscheid wordt gemaakt tussen de in artikel 5 van deze richtlijn genoemde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen.

64. Bovendien varieert de bewaringstermijn van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.

65. Uit het bovenstaande volgt dat richtlijn 2006/24 geen duidelijke en precieze regels bevat betreffende de omvang van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke.

66. Bovendien moet met betrekking tot de regels inzake de beveiliging en de bescherming van de gegevens die worden bewaard door de aanbieders van openbaar beschikbare elektronischecommunicatiediensten of een openbaar communicatienetwerk worden vastgesteld dat richtlijn 2006/24 onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan, zoals wordt vereist door artikel 8 van het Handvest. In de eerste plaats bevat artikel 7 van richtlijn 2006/24 geen specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn

ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

62. En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.

63. En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

64. Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

65. Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

66. De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est

moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen. Bovendien is aan de lidstaten ook geen specifieke verplichting opgelegd om dergelijke regels vast te stellen.

67. Artikel 7 van richtlijn 2006/24, gelezen in samenhang met artikel 4, lid 1, van richtlijn 2002/58 en artikel 17, lid 1, tweede alinea, van richtlijn 95/46, waarborgt niet dat bovengenoemde aanbieders via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden, maar verleent deze aanbieders met name de mogelijkheid om bij de vaststelling van het door hen geboden beschermingsniveau rekening te houden met economische overwegingen, meer bepaald met de kosten voor het uitvoeren van de veiligheidsmaatregelen. In het bijzonder waarborgt richtlijn 2006/24 niet dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd.

68. In de tweede plaats schrijft deze richtlijn niet voor dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest. Een dergelijk toezicht op basis van het Unierecht is evenwel van wezenlijk belang voor de bescherming van personen bij de verwerking van persoonsgegevens (zie in die zin arrest Commissie/Oostenrijk, C-614/10, EU:C:2012:631, punt 37).

69. Gelet op een en ander moet worden geoordeeld dat de wetgever van de Unie met de vaststelling van richtlijn 2006/24 de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest in acht dient te nemen".

2. Als gevolg van dat arrest van het Hof van Justitie heeft het Grondwettelijk Hof bij arrest 84/2015 van 11 juni 2015 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" vernietigd, die ertoe strekte richtlijn 2006/24/EG gedeeltelijk om te zetten.

Het arrest van het Grondwettelijk Hof steunt op de volgende motivering:

"B.10.1. Zoals het Hof van Justitie heeft opgemerkt in de punten 56 en 57 van zijn arrest, schrijft de richtlijn voor om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren, waardoor zij algemeen van toepassing is op alle personen en alle elektronische communicatiemiddelen, zonder onderscheid op basis van het doel, namelijk zware criminaliteit bestrijden, dat de Uniewetgever wilde nastreven.

imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles.

67. L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

68. En second lieu, il convient d'ajouter que ladite directive n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir, en ce sens, arrêt Commission/Autriche, C-614/10, EU:C:2012:631, point 37).

69. Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte".

2. À la suite de cet arrêt de la Cour de justice, l'arrêt 84/2015 du 11 juin 2015 de la Cour constitutionnelle a annulé 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 90*decies* du Code d'instruction criminelle", laquelle avait pour objet d'assurer la transposition partielle de la directive 2006/24/CE.

L'arrêt de la Cour constitutionnelle repose sur la motivation suivante:

"B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre.

De bestreden wet verschilt op dat punt niet van de richtlijn. Zoals in B.8 is vermeld, zijn immers de categorieën van gegevens die moeten worden bewaard identiek aan die welke zijn opgesomd in de richtlijn, terwijl geen enkel onderscheid wordt gemaakt met betrekking tot de betrokken personen of de bijzondere regels die moeten worden bepaald op basis van het doel van bestrijding van de inbreuken beschreven in artikel 126, § 2, van de wet van 13 juni 2005, dat bij de bestreden wet werd vervangen. Net zoals het Hof van Justitie heeft vastgesteld met betrekking tot de richtlijn (punt 58), is de wet dus ook van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met de in de bestreden wet opgesomde inbreuken. Op dezelfde wijze is de wet, zonder enige uitzondering, ook van toepassing op personen van wie de communicaties onder het beroepsgeheim vallen.

B.10.2. Niet méér dan het geval is voor de richtlijn, vereist het bestreden artikel 5 enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Het beperkt evenmin de bewaring van de desbetreffende gegevens 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.

B.10.3. 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.

B.10.4. Wat ten slotte de bewaarperiode van de gegevens betreft, maakt de wet geen enkel onderscheid tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen.

B.11. Om dezelfde redenen als die welke het Hof van Justitie van de Europese Unie ertoe hebben gebracht de "Dataretentierichtlijn" ongeldig te verklaren, dient te worden vastgesteld dat de wetgever, met de aanneming van artikel 5 van de bestreden wet, de grenzen heeft overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Het voormelde artikel 5 schendt bijgevolg de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met die bepalingen. Het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 zijn gegrond.

B.12. Wegens hun ondeelbaar karakter met artikel 5, dienen ook de artikelen 1 tot 4, 6 en 7 van de bestreden wet van 30 juli 2013, en dus de wet in haar geheel, te worden vernietigd".

Het voorliggende voorontwerp strekt ertoe gevolg te geven aan dat arrest 84/2015 van het Grondwettelijk Hof van

La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

B.10.2. Pas plus que ce n'est le cas pour la directive, l'article 5 attaqué ne requiert-il une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Il 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.

B.10.3. 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.

B.10.4. Enfin, 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.

B.11. Par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive "conservation des données" invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

Partant, l'article 5 précité viole les articles 10 et 11 de la Constitution lus en combinaison avec ces dispositions. Le moyen unique dans l'affaire n° 5856 et le premier moyen dans l'affaire n° 5859 sont fondés.

B.12. En raison de leur caractère indissociable avec l'article 5, il y a lieu d'annuler également les articles 1er à 4, 6 et 7 de la loi du 30 juillet 2013 attaquée et donc l'intégralité de ladite loi".

L'avant-projet à l'examen se donne pour objet de faire suite à cet arrêt 84/2015 de la Cour constitutionnelle du

11 juni 2015, dat zelf gevolg geeft aan het arrest van het Hof van Justitie van 8 april 2014.

3. Wat het Europees recht betreft, moet worden opgemerkt dat het arrest van het Hof van Justitie van de Europese Unie, waarbij uitspraak wordt gedaan naar aanleiding van een vraag om de geldigheid van afgeleid recht van de Unie te beoordelen en waarin tot de ongeldigheid van een Europese norm wordt besloten, niet als gevolg heeft dat de ongeldig verklaarde norm uit de rechtsorde verdwijnt, noch dat de normen die eventueel bij de ongeldig verklaarde tekst zijn opgeheven, opnieuw van toepassing worden.

Niettemin moeten alle nationale rechtscolleges zich richten naar het feit dat de ongeldigheid is vastgesteld,[1] moeten de overheden van de Unie de ongeldig verklaarde handeling wijzigen of opheffen en moeten de nationale overheden, met inachtneming van de nationale procedures, de eigen regels wijzigen of opheffen die ingevolge de ongeldig verklaarde handeling zijn vastgesteld.[2]

Aangezien richtlijn 2006/24/EG, die de verschillende wetgevingen van de lidstaten over de bewaring van de gegevens betreffende elektronische communicatie onderling in overeenstemming beoogde te brengen, ongeldig is verklaard, mag niet de richtlijn, maar enkel het recht dat vóór de inwerkingtreding van de richtlijn van toepassing was, in aanmerking genomen worden, niettegenstaande de bevoegde overheden van de Europese Unie die richtlijn nog niet hebben opgeheven of gewijzigd.

Wat dat betreft, moet rekening worden gehouden met artikel 15 van richtlijn 2002/85/EG van het Europees Parlement en de Raad van 12 juli 2002 “betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)” (hierna

1 Waarbij die rechtscolleges zich eventueel opnieuw tot het Hof moeten wenden indien er nog twijfels zijn over wat die ongeldigheid precies inhoudt.

2 Zie hierover C. Soulard, A. Rigaux, D. Simon en R. Munoz, “*Contentieux de l’Union européenne. Renvoi préjudiciel, recours en manquement / 3”*, Parijs, Lamy & Wolters Kluwer France, 2011, 108 e.v.

11 juin 2015, lequel fait lui-même suite à l’arrêt de la Cour de justice du 8 avril 2014.

3. Au regard du droit européen, il y a lieu d’observer que l’arrêt de la Cour de justice de l’union européenne qui se prononce sur une question en appréciation en validité du droit dérivé de l’Union, et conclut à l’invalidité d’une norme européenne, n’a pas pour effet de faire disparaître de l’ordre juridique la norme invalidée, ni de faire revivre les normes éventuellement abrogées par le dispositif invalidé.

Il n’en reste pas moins que l’ensemble des juridictions nationales sont liées par le constat d’invalidité[1], que les autorités de l’Union ont, elles, l’obligation de modifier ou d’abroger l’acte invalidé et que les autorités nationales ont celle de modifier ou d’abroger les règles nationales qui ont été adoptées en suite de l’acte invalidé en respectant les procédures nationales[2].

Par conséquent, dès lors qu’est invalidée la directive 2006/24/CE, qui avait pour objet d’harmoniser les différentes législations des États membres relatives à la conservation des données en matière de communications électroniques et, même si cette directive n’a pas encore été abrogée ou modifiée par les autorités compétentes de l’Union européenne, il n’y a pas lieu d’y avoir égard mais seul le droit applicable avant son entrée en vigueur doit être pris en considération.

À ce propos, il faut tenir compte de l’article 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 “concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)” (ci-après la

1 À charge éventuellement pour celles-ci d’interroger à nouveau la Cour si des doutes subsistent sur la portée exacte de l’invalidité.

2 Voir, sur ces questions, *“Contentieux de l’Union européenne. Renvoi préjudiciel, recours en manquement/3”*, sous la direction de C. Soulard, A. Rigaux, D. Simon et R. Munoz, Paris, éditions Lamy, Wolters-Kluwer France, 2011 pp. 108 et s.

richtlijn 2002/58/EG genoemd), zoals dat van toepassing was voordat het bij richtlijn 2006/24/EG is gewijzigd.[3]

Dat artikel 15 luidde als volgt:

"Artikel 15

Toepassing van een aantal bepalingen van Richtlijn 95/46/EG

1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6,

directive 2002/58/CE), tel qu'il était en vigueur avant sa modification par la directive 2006/24/CE[3].

Cet article 15 disposait comme suit:

"Article 15

Application de certaines dispositions de la directive 95/46/CE

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations

[3] Wat betreft de vraag of het recht van de Europese Unie en meer bepaald het Handvest van de grondrechten van de Europese Unie toepasselijk is op de maatregelen inzake de bewaring van metagegevens die met het oog op de openbare veiligheid, de landsverdediging en de staatsveiligheid door de lidstaten worden genomen, moet rekening worden gehouden met de artikelen 72 en 73 van het Verdrag betreffende de werking van de Europese Unie. Die bepalingen bevinden zich in titel V van het derde deel van het Verdrag, betreffende de ruimte van vrijheid, veiligheid en recht. Artikel 72 bepaalt dat "[d]eze titel ( ) de uitoefening van de verantwoordelijkheid van de lidstaten voor de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid onverlet [laat]", terwijl artikel 73 bepaalt dat "[h]et ( ) de lidstaten vrij[staat] onderling en onder hun verantwoordelijkheid vormen van samenwerking en coördinatie te organiseren zoals zij het passend achten tussen hun bevoegde overheidsdiensten die verantwoordelijk zijn voor het verzekeren van de nationale veiligheid". De Raad van State van Frankrijk heeft evenwel opgemerkt dat het afgeleid recht van de Unie dienaangaande soms complexer blijkt te zijn. Zo stelt hij in verband met artikel 15 van richtlijn 2002/58/EG, in "Les rapports du Conseil d'état – Le numérique et les droits fondamentaux" het volgende: "( ) tant la directive n° 95/46/CE que la directive n° 2002/58/CE excluent de leur champ la matière pénale et les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'État. Et l'existence de ces actes, mettant en œuvre le droit de l'Union, est une condition d'application de la Charte. La directive n° 2002/58/CE est cependant ambiguë à cet égard: si son article 1.3 restreint son champ d'application, son article 15.1 dispose que les États ne peuvent déroger aux droits garantis par la directive pour les finalités énumérées ci-dessus que s'il s'agit de mesures nécessaires et proportionnées, prises dans le respect des "principes généraux du droit communautaire". Il traite en particulier de la conservation des données, en prévoyant que "les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié" par l'une des finalités énumérées ci-dessus. Il est donc possible de soutenir que la directive n° 2002/58/CE régit les législations des États relatives à la conservation des métadonnées. Les usages des métadonnées en matière de sécurité nationale échappent au champ d'application du droit de l'Union, mais la conservation porte atteinte par elle-même, indépendamment de l'usage, aux droits garantis par la directive, puisque l'article 5 impose en principe l'effacement des données. En outre, si la proposition de directive relative à la protection des données personnelles en matière pénale était adoptée, les traitements de données personnelles à des fins de police judiciaire entreraient pleinement dans le champ du droit de l'Union européenne. Dès lors, en raison de l'ambiguïté du champ d'application de la directive n° 2002/58/CE, la question de la conformité de la législation nationale à la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été interprétée par la C.J.U.E. dans l'arrêt Digital Rights Ireland, reste posée" (http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf, 199-200).

[3] Sur la question de savoir si le droit de l'Union européenne et plus spécialement la Charte des droits fondamentaux est d'application pour les mesures prises par les États membres en matière de conservation de métadonnées dans un but de sécurité publique, la défense et la sûreté de l'État, il faut avoir égard aux articles 72 et 73 du Traité sur le fonctionnement de l'Union européenne, dispositions figurant sous le Titre V de la troisième partie du Traité, relatif à l'espace de liberté, de sécurité et de justice; l'article 72 dispose que "[l]e présent titre ne porte pas atteinte à l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure", tandis que l'article 73 prévoit qu' "[i]l est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale". Toutefois, comme le relève le Conseil d'État de France, le droit dérivé de l'Union s'avère parfois plus complexe sur cette question. Ainsi, s'agissant de l'article 15 de la directive 2002/58/CE, le Conseil d'État de France, dans un document intitulé "Les rapports du Conseil d'État – Le numérique et les droits fondamentaux" a exposé ce qui suit: "[...] tant la directive n° 95/46/CE que la directive n° 2002/58/CE excluent de leur champ la matière pénale et les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'État. Et l'existence de ces actes, mettant en œuvre le droit de l'Union, est une condition d'application de la Charte. La directive n° 2002/58/CE est cependant ambiguë à cet égard: si son article 1.3 restreint son champ d'application, son article 15.1 dispose que les États ne peuvent déroger aux droits garantis par la directive pour les finalités énumérées ci-dessus que s'il s'agit de mesures nécessaires et proportionnées, prises dans le respect des "principes généraux du droit communautaire". Il traite en particulier de la conservation des données, en prévoyant que "les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié" par l'une des finalités énumérées ci-dessus. Il est donc possible de soutenir que la directive n° 2002/58/CE régit les législations des États relatives à la conservation des métadonnées. Les usages des métadonnées en matière de sécurité nationale échappent au champ d'application du droit de l'Union, mais la conservation porte atteinte par elle-même, indépendamment de l'usage, aux droits garantis par la directive, puisque l'article 5 impose en principe l'effacement des données. En outre, si la proposition de directive relative à la protection des données personnelles en matière pénale était adoptée, les traitements de données personnelles à des fins de police judiciaire entreraient pleinement dans le champ du droit de l'Union européenne. Dès lors, en raison de l'ambiguïté du champ d'application de la directive n° 2002/58/CE, la question de la conformité de la législation nationale à la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été interprétée par la C.J.U.E. dans l'arrêt Digital Rights Ireland, reste posée", http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf, pp. 199-200.

artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

1*ter*. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.[4]

2. Het bepaalde in hoofdstuk III van Richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

3. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van Richtlijn 95/46/EG, voert de in artikel 30 van die richtlijn vermelde taken ook uit ten aanzien van aangelegenheden die onder de onderhavige richtlijn vallen, namelijk de bescherming van de fundamentele rechten en vrijheden en van rechtmatige belangen in de sector elektronische communicatie".

4. Wat het interne recht betreft, worden de bepalingen van de wet van 30 juli 2013, zoals in de memorie van toelichting van het voorliggende voorontwerp wordt onderstreept, geacht nooit te hebben bestaan, aangezien ze vernietigd zijn, en worden de bepalingen die bij die wet zijn opgeheven opnieuw toepasselijk.

Als gevolg van de vernietiging van de wet van 30 juli 2013 is meer bepaald de versie van artikel 126 van de wet van 13 juni 2005 "betreffende de elektronische communicatie"[5]

[4] Lid ingevoegd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 "tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming".

[5] Hierna "de wet van 13 juni 2005" genoemd.

prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

1*ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse[4].

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques".

4. Concernant le droit interne, comme le souligne l'exposé des motifs relatif à l'avant-projet à l'examen, dès lors que les dispositions de la loi du 30 juillet 2013 ont été annulées, elles sont censées ne jamais avoir existé et les dispositions abrogées par cette loi redeviennent applicables.

Plus spécialement, à la suite de l'annulation de la loi du 30 juillet 2013, l'article 126 de la loi du 13 juin 2005 "relative aux communications électroniques"[5], est d'application tel

[4] Paragraphe inséré par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 "modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs'.

[5] Ci-après "la loi du 13 juin 2005".

toepasselijk die vóór de inwerkingtreding van de wet van 30 juli 2013 van kracht was en die luidt als volgt:

"§ 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning 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 voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.

De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België".

Volgens de memorie van toelichting bij de ontworpen tekst "schenkt" het hierboven weergegeven artikel 126 "geen voldoening".

5. In die context beoogt de steller van het voorontwerp derhalve niet meer de richtlijn om te zetten die het Hof van Justitie ongeldig heeft verklaard, maar wil veeleer een regeling voor gegevensbewaring invoeren die de doelstellingen dient die het Hof van Justitie en het Grondwettelijk Hof legitiem hebben geacht en die in overeenstemming is met het dictum en de motivering van de beslissingen van die hoge rechtscolleges.

Bovendien moet worden opgemerkt dat in de ontworpen tekst, evenals in het geldende artikel 126 en in het artikel 126 dat bij arrest 84/2015 van het Grondwettelijk Hof is vernietigd, wordt voorgeschreven dat gegevens worden bewaard met een doel dat verder gaat dan de doelstellingen waarin richtlijn 2006/24/EG voorziet en die bestaan in "het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten".

Zo bijvoorbeeld zullen de te bewaren gegevens aan de bevoegde overheden worden meegedeeld met het oog op welbepaalde doeleinden, waaronder inzonderheid de identificatie van de personen die een hulpdienst hebben opgeroepen zodat de dienst in kwestie tijdig kan handelen, de opsporing van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, of de identificatie van de persoon die kwaadwillig

qu'il était en vigueur avant l'entrée en vigueur de la loi du 30 juillet 2013, qui dispose comme suit:

"§ 1er. Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique".

L'exposé des motifs relatif au texte en projet mentionne à ce propos que l'article 126 reproduit ci-avant n'est pas "satisfaisant".

5. Dans ce contexte, l'auteur de l'avant-projet entend dès lors adopter un dispositif qui n'a plus pour objet de transposer la directive invalidée par la Cour de Justice, mais bien plutôt de mettre en place un système de conservation des données qui permettraient d'atteindre les objectifs dont la Cour de justice et la Cour constitutionnelle ont reconnu le caractère légitime, tout en se conformant aux décisions de ces hautes juridictions, dans leur dispositif et leur motivation.

Il convient en outre de relever que comme l'article 126 en vigueur, ainsi que l'article 126 annulé par l'arrêt 84/2015 de la Cour constitutionnelle, le dispositif en projet impose la conservation de données dans des buts qui dépassent les finalités prévues par la directive 2006/24/CE, à savoir "des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne".

Ainsi, les données dont la conservation est imposée seront communiquées aux autorités habilitées, à des fins déterminées, fins parmi lesquelles figurent notamment l'identification des personnes ayant fait appel à un service d'urgence, en vue de permettre l'intervention du service concerné dans un délai utile, la 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, ou encore, l'identification de la

gebruik heeft gemaakt van een netwerk of een dienst voor elektronische communicatie.[6]

Hetzelfde geldt voor de doeleinden die de ontworpen tekst vermeldt betreffende het voorkomen en bestraffen van criminaliteit in het algemeen, betreffende de gevaren voor het menselijk leven of voor de fysieke integriteit van personen en goederen, of betreffende het onrechtmatige gebruik van systemen voor elektronische communicatie, en die in de lijn liggen van de doelstellingen die in artikel 15 van richtlijn 2002/58/EG worden opgenoemd.

II. BEPALINGEN INGEVOERD BIJ DE ONTWORPEN TEKST OM TEGEMOET TE KOMEN AAN DE VEREISTEN WAARAAN VOLGENS DE ARRESTEN VAN HET HOF VAN JUSTITIE EN VAN HET GRONDWETTELIJK HOF VOLDAAN MOET ZIJN

1. Uit het arrest van het Hof van Justitie, waarop het arrest van het Grondwettelijk Hof aansluit, moet voornamelijk het volgende worden onthouden:

1° De bewaring van gegevens met de bedoeling dat de bevoegde nationale overheden eventueel tot die gegevens toegang hebben, zoals richtlijn 2006/24/EG voorschrijft, vormt een inmenging in het fundamentele recht op eerbiediging van de persoonlijke levenssfeer en in de andere rechten die zijn neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, met als verzwarende omstandigheid dat de overheden kennis moeten kunnen nemen van die gegevens.

2° De wezenlijke inhoud van die rechten kan evenwel niet door die inmenging worden aangetast, aangezien artikel 1, lid 2, van richtlijn 2006/24/EG niet toestaat dat van de inhoud zelf van de elektronische communicatie kennis wordt genomen.

3° Die inmenging beantwoordt voorts aan een doelstelling van algemeen belang, namelijk de bestrijding van het internationale terrorisme, de bestrijding van de zware criminaliteit met het oog op de openbare veiligheid en het recht van eenieder op veiligheid, en bewaring van de gegevens in kwestie kan worden beschouwd als een geschikt middel om de doelstelling te verwezenlijken die richtlijn 2006/24/EG nastreeft.

4° De vraag rijst dus of de beoogde inmenging evenredig is met het nagestreefde doel, namelijk of het gaat om maatregelen die absoluut noodzakelijk zijn om dat doel te bereiken. Wat dat betreft moet de regeling in kwestie “duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens”.

Dienaangaande moet het volgende in aanmerking worden genomen.

6 Ontworpen artikel 126, § 2.

personne ayant effectué une utilisation malveillante d’un réseau ou d’un service de communications électroniques[6].

Ainsi en va-t-il aussi des finalités reprises au texte en projet, qui concernent la prévention et la répression de la criminalité en général, les risques pour la vie humaine ou l’intégrité physique des personnes et des biens, ou encore les utilisations non autorisées du système de communications électroniques, qui s’inscrivent dans les finalités énumérées à l’article 15 de la directive 2002/58/CE.

II. MISE EN ŒUVRE, PAR LE TEXTE EN PROJET, DES EXIGENCES DÉCOULANT DES ARRÊTS DE LA COUR DE JUSTICE ET DE LA COUR CONSTITUTIONNELLE

1. À la lecture de l’arrêt de la Cour de justice, dans le prolongement duquel est intervenu l’arrêt de la Cour constitutionnelle, il y a lieu de retenir essentiellement ce qui suit:

1° La conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d’un accès éventuel à celles-ci, telle qu’imposée par la directive 2006/24/CE, constitue une ingérence dans le droit fondamental au respect de la vie privée et les autres droits consacrés à l’article 7 et à l’article 8 de la Charte des droits fondamentaux de l’Union européenne, aggravée par la circonstance que les autorités pourront prendre connaissance de ces données.

2° Cette ingérence n’est toutefois pas de nature à porter atteinte au contenu essentiel de ces droits, étant donné que, ainsi qu’il découle de son article 1er, paragraphe 2, cette directive 2006/24/CE ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

3° Cette ingérence répond par ailleurs à un objectif d’intérêt général, étant la lutte contre le terrorisme international, la lutte contre la criminalité grave afin de garantir la sécurité publique et le droit de toute personne à la sûreté, et la conservation des données concernées peut être considérée comme apte à réaliser l’objectif poursuivi par cette directive 2006/24/CE.

4° La question se pose dès lors de savoir si l’ingérence prévue est proportionnée au but poursuivi, à savoir si elle comprend les mesures strictement nécessaires pour atteindre ce but; à ce propos, la réglementation en cause “doit prévoir des règles claires et précises régissant la portée et l’application de la mesure en cause et imposant un minimum d’exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d’abus ainsi que contre tout accès et toute utilisation illicites de ces données”.

Sur ce point, il faut avoir égard aux éléments suivants.

6 Article 126, § 2, en projet.

1° Het feit dat de regeling algemeen van toepassing is op alle personen, alle middelen voor elektronische communicatie en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking word gesteld of enige uitzondering wordt gemaakt op basis van het doel zware criminaliteit te bestrijden. Dat blijkt uit het volgende:

a) enerzijds schrijft de regeling niet voor dat de personen van wie de gegevens worden bewaard zich, zelfs niet indirect, in een situatie moeten bevinden die aanleiding kan geven tot strafrechtelijke vervolging, en bevat ze geen uitzonderingen, zodat ze zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het beroepsgeheim vallen;

b) anderzijds schrijft de regeling niet voor dat er een verband moet bestaan tussen de te bewaren gegevens en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.

2° Het feit dat de regeling niet alleen geen beperkingen oplegt, maar ook “geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen”. Wat dat betreft, bevat de regeling “[niet de desbetreffende] materiële en procedurele voorwaarden” en “bepaalt [ze] niet uitdrukkelijk dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen”. Er zijn inzonderheid “geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel”, en “de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens [is] niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten”.

3° Het feit dat de gegevens gedurende een termijn van ten minste zes maanden moeten worden bewaard “zonder dat enig onderscheid wordt gemaakt tussen de (…) categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen”. “Bovendien varieert de bewaringstermijn van ten minste zes

1° Au fait que la réglementation couvre de manière généralisée toute personne et tous les moyens de communications électroniques ainsi que l’ensemble des données relatives au trafic sans qu’aucune différenciation, limitation ni exception soient opérées en fonction de l’objectif de lutte contre les infractions graves; ainsi,

a) d’une part, la réglementation n’impose pas que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales et elle ne prévoit aucune exception, de sorte qu’elle s’applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel;

b) d’autre part, la réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n’est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d’être mêlées d’une manière ou d’une autre à une infraction grave, soit sur des personnes qui pourraient, pour d’autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d’infractions graves.

2° Au fait que, à cette absence générale de limites, s’ajoute la circonstance que la réglementation “ne prévoit aucun critère objectif permettant de délimiter l’accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l’ampleur et de la gravité de l’ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence”; à cet égard, la réglementation “ne contient pas les conditions matérielles et procédurales y afférentes” et “ne dispose pas expressément que cet accès et l’utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d’infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci”; spécialement, il n’est prévu “aucun critère objectif permettant de limiter le nombre de personnes disposant de l’autorisation d’accès et d’utilisation ultérieure des données conservées au strict nécessaire au regard de l’objectif poursuivi” et “l’accès aux données conservées par les autorités nationales compétentes n’est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l’accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d’atteindre l’objectif poursuivi et intervient à la suite d’une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales”.

3° Au fait que s’agissant de la durée de conservation des données, la conservation des données pendant une période d’au moins six mois est prévue “sans que soit opérée une quelconque distinction entre les catégories de données […] en fonction de leur utilité éventuelle aux fins de l’objectif poursuivi ou selon les personnes concernées”; “[c]ette durée se situe,

maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is".

Derhalve kan, volgens het Hof van Justitie, niet worden aangenomen "dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke".

Bovendien,

4° is er niet voorzien in "specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen". Er wordt van de aanbieders meer bepaald niet vereist dat ze "via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden": er wordt inzonderheid niet gewaarborgd dat "de gegevens na de bewaarperiode onherroepelijk worden vernietigd".

5° wordt nergens voorgeschreven dat de gegevens in kwestie op het grondgebied van de Unie moeten worden bewaard, zodat "niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest".

2. Hoewel de doelstellingen die het voorliggende voorontwerp nastreeft, verder reiken dan die van richtlijn 2006/24/EG dat door het Hof van Justitie ongeldig is verklaard, blijkt niet, zoals hierboven is uiteengezet, niet dat elk van die doelen legitiem zou zijn en, meer bepaald, dat ze niet in overeenstemming zouden kunnen zijn met artikel 15, lid 1, van richtlijn 2002/58/EG.

Bij het onderzoek van het voorontwerp van wet moet dus rekening worden gehouden met de omstandigheid dat de vereisten waaraan volgens het arrest van het Hof van Justitie voldaan moet zijn, betrekking hebben op de bewaring van en de daaropvolgende toegang tot gegevens zoals bedoeld in richtlijn 2006/24/EU, namelijk de bewaring en de toegang tot gegevens "teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit". De strekking van het arrest van het Hof en de gevolgtrekkingen die daaruit moeten worden gemaakt, hoe strikt deze ook zijn, hebben dus enkel betrekking op het bewaren van gegevens waarvan het uiteindelijke doel erin bestaat gedragingen en handelingen die zware overtredingen vormen, strafrechtelijk te bestraffen, wat per definitie geen lichte bestraffing kan zijn.

De strekking van dat arrest kan dus *a priori* niet worden uitgebreid tot een bewaring van gegevens of een toegang tot bewaarde gegevens die andere doeleinden zouden dienen, zoals het opsporen door een ombudsdienst van een persoon

en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire".

Il en résulte que, selon la Cour de justice, l'on ne peut considérer que l'"ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire".

En outre,

4° Il n'est pas prévu de "règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité"; plus spécialement, il n'est pas imposé aux fournisseurs "un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles": en particulier, rien ne garantit la "destruction irrémédiable des données au terme de la durée de conservation de celles-ci".

5° Rien n'impose que les données en cause soient conservées sur le territoire de l'Union, de sorte "qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents".

2. Comme exposé ci-avant, si l'avant-projet à l'examen, dans les finalités qu'il poursuit, est plus large que la directive 2006/24/UE invalidée par la Cour de Justice, il n'apparaît pas que les buts poursuivis par le texte en projet ne seraient pas tous et chacun légitimes, et notamment qu'ils ne pourraient pas être poursuivis conformément à l'article 15, paragraphe 1er, de la directive 2002/58/CE.

L'avant-projet de loi doit donc être examiné en tenant compte de la circonstance que les exigences qui résultent de l'arrêt de la Cour de justice concernent la conservation et l'accès subséquent à des données, telles que visées par la directive 2006/24/UE, à savoir la conservation et l'accès à des données "en vue de garantir la disponibilité [de celles-ci] à des fins de recherche, de détection et de poursuite d'infractions graves": la portée de l'arrêt de la Cour et des conséquences à en tirer, aussi rigoureuses soient-elles, sont donc limitées à une conservation de données dont la finalité est, en sa phase ultime, la sanction pénale, par hypothèse, nécessairement non anodine, de comportements et d'actes constitutifs d'infractions graves.

Rien ne permet, *a priori*, d'étendre la portée de cet arrêt à une conservation ou à un accès à des données conservées qui auraient d'autres finalités comme la recherche, par un service de médiation, de l'auteur d'appels malveillants,

die kwaadwillige oproepen pleegt, de identificatie van de persoon die een hulpdienst belt of van de plaats van waaruit zo'n oproep wordt gedaan zodat de hulpdienst kan optreden en kan zorgen voor de bescherming van goederen en personen, of het opsporen buiten iedere strafrechtelijke context van een persoon van wie de verdwijning onrustwekkend is wanneer blijkt dat zijn leven in onmiddellijk gevaar zou kunnen zijn. De strekking van het arrest kan zelfs niet tot de activiteiten van de inlichtingendiensten worden uitgebreid.

Deze laatste gevallen zullen dus alleen worden onderzocht in het licht van het recht op eerbiediging van het privéleven dat bij artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en bij artikel 22 van de Grondwet is gewaarborgd.[7]

3. Gelet op het aldus in herinnering gebrachte juridisch kader, geeft de ontworpen tekst aanleiding tot de volgende algemene opmerkingen.

3.1. Het feit dat de ontworpen tekst in het algemeen betrekking heeft op alle personen, zonder dat enig onderscheid wordt gemaakt tussen personen, periode en geografische zone en zonder dat vereist is dat enig verband bestaat tussen de gegevens die zouden worden bewaard en een bedreiging van de openbare veiligheid

3.1.1. In de memorie van toelichting wordt in dat verband melding gemaakt van het volgende:

"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.

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

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

[7] Zie onder meer L. Tassone, "La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme" in A. Grosjean (ed.), *Enjeux européens et mondiaux de la protection des données personnelles*, verzamelwerk, Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42 178/2, op 19 februari 2007 gegeven over een voorontwerp dat ontstaan gegeven heeft aan de wet van 4 februari 2010 "betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten' (*Parl.St.* Senaat 2006-07, nr. 3-2138/1, 279-297).

l'identification de l'appelant ou du lieu d'un appel aux service d'urgence, en vue de permettre à ceux-ci d'intervenir afin de pouvoir garantir la sauvegarde des biens et des personnes, ou la recherche, indépendante de tout contexte infractionnel, d'une personne dont la disparition est inquiétante et dont il apparaît que la vie pourrait être en danger imminent, ni même aux activités des services de renseignements.

Ces dernières hypothèses ne seront donc examinées qu'au regard du droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 22 de la Constitution[7].

3. Compte tenu du contexte ainsi rappelé, le texte en projet appelle les observations générales suivantes.

3.1. Quant au fait que le texte en projet couvre de manière généralisée toute personne, sans distinction entre personnes, période temporelle et zone géographique, et sans qu'une relation soit requise entre les données dont la conservation est prévue et une menace pour la sécurité publique

3.1.1. À cet égard, l'exposé des motifs mentionne ce qui suit:

"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.

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

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'ensuit 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

[7] Voir e.a., L. Tassone, *"La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme"* in "Enjeux européens et mondiaux de la protection des données personnelles", ouvrage collectif sous la direction d'A. Grosjean, Larcier, coll. Création Information Communication, p. 53 et s., et les références citées; concernant les services de renseignement et de sécurité, voir e.a. l'avis 42 178/2 donné le 19 février 2007 sur un avant-projet devenu la loi du 4 février 2010 "relative aux méthodes de recueil des données par les services de renseignement et de sécurité" (*Doc. parl.*, Sénat, 2006-2007, n° 3-2138/1, pp. 279-297).

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.

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 criminele 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.

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.

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 criminel.

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 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 l'étranger exigent le passage par la coopération judiciaire formelle pour transmettre des données. Or le passage par la coopération judiciaire, notamment avec les États-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.

[…]

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 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.

[…] 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 […] een *a priori* differentiatie van dit element niet mogelijk is.

De Commissie [voor de bescherming van de persoonlijke levenssfeer] is dezelfde mening toegedaan, aangezien zij er in […] advies 33-2015 met betrekking tot de ontworpen tekst op wijst dat “bepaalde aspecten van [de] arresten [van het Hof van justitie en het grondwettelijke Hof] de Commissie evenwel moeilijk toepasbaar [lijken] te zijn, in het bijzonder het onderscheid op grond van personen, periodes en/of geografische zones”.

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.

[…]

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 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.

[…] 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.

Dans l’avis 33-2015 [relatif au texte en projet], la Commission [de la protection de la vie privée] va dans le même sens puisqu’elle indique que “certains aspects des arrêts [de la Cour de justice et de la Cour constitutionnelle] lui paraissent difficilement applicables, en particulier la distinction en fonction des personnes, périodes temporelles et/ou zones géographiques”.

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.

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 décharge kan meespelen.

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.

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.

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) 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.

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 (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). 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.

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".

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.

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.

Verder in de tekst zal evenwel blijken dat 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.

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.

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

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 exemple en matière de pédopornographie) et, d'autre part, la 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). 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) 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".

Ici aussi, on s'est interrogé sur la possibilité de créer une différenciation 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.

Cette différenciation 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.

On verra toutefois plus loin que la protection de certaines professions est bien renforcée dans le présent projet de loi mais au niveau de la réglementation de l'accès aux données conservées.

On peut conclure qu'il n'est pas possible de modaliser l'article 126 LCE sur base du premier élément (l'absence de différenciation 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.

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

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.

In voormeld advies over onderhavig wetsontwerp steunt de Commissie deze interpretatie en stelt ze: "evenwel wordt, zoals de Memorie van toelichting aangeeft, in geen van beide arresten geconcludeerd dat slechts één van de vier elementen volstaat om een schending van het evenredigheidsbeginsel in te houden. Indien een bepaald element van de arresten niet kan worden weerhouden, dient dit gecompenseerd te worden door een striktere regeling inzake de andere aspecten."

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."

3.1.2. In verband met de onmogelijkheid om alleen gegevens aangaande bepaalde personen, of aangaande bepaalde groepen van personen te bewaren, meer bepaald aangaande personen die al betrokken zouden zijn bij een onderzoek, welke onmogelijkheid eveneens vastgesteld is door de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies over de ontworpen tekst, is het de afdeling Wetgeving niet duidelijk om welke redenen de in de memorie van toelichting gegeven verantwoording in twijfel zou kunnen worden getrokken. Bijvoorbeeld, indien voor de operatoren en de aanbieders geen enkele algemene verplichting zou gelden tot bewaring van gegevens, zou de regeling die daarvan het gevolg zou zijn impliceren dat de bewaring van en de toegang tot de gegevens alleen *a posteriori* mogelijk zouden zijn, terwijl de overheid geen toegang zou kunnen hebben tot de gegevens uit het verleden (of de *a priori*-gegevens) die nochtans noodzakelijk of zelfs onontbeerlijk zijn voor het halen van de legitieme doelstellingen bepaald in de ontworpen tekst.

Zo ook is het, in verband met een eventuele beperking van de bewaringsplicht tot een bepaalde geografische zone of een bepaalde periode, voor de afdeling Wetgeving niet duidelijk om welke redenen de in de memorie van toelichting gevolgde redenering in twijfel zou kunnen worden getrokken. Wat deze laatste twee beperkingen betreft, rijst evenwel de vraag of niet zou kunnen worden overwogen om, zonder afbreuk te doen aan de nagestreefde legitieme doelstellingen, een kortere algemene bewaartermijn te bepalen en tegelijk een regeling in te voeren waarbij de Koning, mits voorzien wordt in bepaalde procedurele waarborgen,[8] zou kunnen worden gemachtigd om in objectieve omstandigheden van een specifieke potentiële bedreiging die nauwkeurig moeten worden afgebakend, de

[8] Bijvoorbeeld bij een besluit vastgesteld na overleg in de Ministerraad dat vooraf voor advies is voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer en aan het Instituut.

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.

Dans son avis précité sur le présent projet de loi, la Commission vie privée soutient cette interprétation et indique: "comme indiqué dans l'Exposé des Motifs, aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects".

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".

3.1.2. Concernant l'impossibilité – constatée également par la Commission pour la protection de la vie privée dans son avis sur le texte en projet – de limiter la conservation des données à certaines personnes, ou à certains groupes de personnes, notamment celles qui feraient déjà l'objet d'une enquête, la section de législation n'aperçoit pas les raisons qui seraient susceptibles de remettre en question les justifications données dans l'exposé des motifs. Ainsi, si aucune obligation de conservation n'était imposée de manière générale aux opérateurs et fournisseurs, le système qui en résulterait impliquerait que seuls une conservation et un accès aux données *a posteriori* seraient possibles, sans que l'autorité puisse avoir accès aux données passées (ou *a priori*), qui sont pourtant nécessaires, voire indispensables, à la réalisation des objectifs légitimes prévus par le texte en projet.

De même, concernant une éventuelle limitation de l'obligation de conservation à une zone géographique ou à une période temporelle déterminée, la section de législation n'aperçoit pas les raisons qui seraient susceptibles de remettre en question le raisonnement figurant dans l'exposé des motifs. Quant à ces deux dernières limitations, la question se pose toutefois de savoir s'il ne serait pas envisageable, sans nuire aux objectifs légitimes poursuivis, de définir un délai général de conservation plus restreint, tout en mettant en place un système dans lequel moyennant certaines garanties procédurales[8], le Roi pourrait être habilité, dans des circonstances objectives de menace potentielle spécifique à définir avec précision, à étendre le délai de conservation des données

[8] Par exemple, un arrêté délibéré en Conseil des ministres, soumis préalablement à l'avis de la Commission pour la protection de la vie privée et à celui de l'Institut.

bewaartermijn van de gegevens te verlengen (waarbij de wetgever evenwel een bovengrens vaststelt voor die verlenging van de termijn) en om, in voorkomend geval, gelet op de aard of de omvang van de bedreiging, meteen ook een bepaalde geografische zone af te bakenen.

Wat, ten slotte, de beperking betreft tot bepaalde beroepen in het kader van de beoefening waarvan een beroepsgeheim geldt, kan los van de in de memorie van toelichting vermelde gegevens niet worden uitgesloten dat de beoefenaars van deze beroepen dezelfde dienst voor elektronische communicatie gebruiken zowel voor privécommunicaties, of in het algemeen voor communicaties die niet onder het beroepsgeheim vallen, als voor communicaties die wel onder het beroepsgeheim vallen. Gelet op die mogelijkheid, komt het er dus niet zozeer op aan te voorzien in een beperking van de te bewaren gegevens, maar te voorkomen dat die gegevens worden bekendgemaakt in omstandigheden die, voor zover het gaat om gegevens die onder het beroepsgeheim vallen, niet in overeenstemming zouden zijn met de beginselen ter zake.

3.1.3. Hoewel er duidelijk logica zit in de redenen waarom de steller van het voorontwerp verklaart dat het hem onmogelijk is tegemoet te komen aan de meest strikte uitlegging van de hier bedoelde vereisten, neemt zulks niet weg dat de ontworpen tekst er per definitie niet toe strekt aan die vereisten te voldoen, wat het dispositief blootstelt aan kritiek.

De mate waarin het dispositief aan kritiek blootstaat, hangt evenwel af van de draagwijdte die dient te worden toegekend aan de arresten in kwestie en dan vooral aan het arrest van het Hof van Justitie.

Wat het laatstgenoemde arrest betreft, heeft de Raad van State van Frankrijk het volgende opgemerkt:

"L'arrêt *Digital Rights Ireland*, dont la Cour n'a pas différé les effets, soulève deux questions: celle de la possibilité de continuer à appliquer les législations nationales sur la conservation des données et celle du cadre qui devrait être défini pour se substituer à la directive n° 2006/24/CE. Les deux questions procèdent en réalité d'une même interrogation sur l'interprétation de l'arrêt. De manière schématique, deux lectures peuvent en être faites: celle d'une condamnation de l'insuffisance des garanties prévues par la directive; celle d'une condamnation de tout système de conservation générale des métadonnées, quel qu'il soit.

[…]

La première interprétation de cet arrêt peut se fonder sur le fait que la Cour a fait masse de trois éléments pour juger que le principe de proportionnalité était méconnu, et que le second avait trait à l'absence de toute précision sur les conditions d'accès des États aux métadonnées conservées par les opérateurs.

Selon cette interprétation, si la directive avait fixé des garanties concernant l'accès, l'appréciation de la Cour aurait peut-être été différente. Elle aurait également pu être influencée par l'existence de restrictions concernant la conservation, par exemple une durée maximale plus courte que celle de

(le législateur fixant toutefois une limite à cette extension de délai), tout en définissant, le cas échéant, compte tenu de la nature ou de l'étendue de la menace, une zone géographique déterminée.

Enfin, s'agissant de la limitation à certaines professions dont l'exercice fait l'objet d'un secret professionnel, outre les éléments mentionnés dans l'exposé des motifs, l'on ne peut exclure que les titulaires de ces professions utilisent le même service de communications électroniques pour des communications tant privées ou, de manière générale, non couvertes par le secret professionnel, que pour des communications couvertes par le secret professionnel. Compte tenu de cette possibilité, l'essentiel est donc non pas de limiter la conservation des données mais d'éviter qu'elles soient divulguées dans des conditions qui, pour celles couvertes par le secret professionnel, ne seraient pas conformes aux principes en la matière.

3.1.3. Si l'on comprend la logique des raisons pour lesquelles l'auteur de l'avant-projet se déclare dans l'impossibilité de donner suite à la lecture la plus stricte des exigences ici visées, il reste que, par hypothèse, le texte en projet envisage de ne pas répondre à ces exigences, ce qui en fragilise le dispositif.

Cette fragilité est toutefois fonction de la portée qu'il convient de conférer aux arrêts concernés, et surtout, à celui de la Cour de justice.

Concernant ce dernier, le Conseil d'État de France a relevé ce qui suit:

"L'arrêt *Digital Rights Ireland*, dont la Cour n'a pas différé les effets, soulève deux questions: celle de la possibilité de continuer à appliquer les législations nationales sur la conservation des données et celle du cadre qui devrait être défini pour se substituer à la directive n° 2006/24/CE. Les deux questions procèdent en réalité d'une même interrogation sur l'interprétation de l'arrêt. De manière schématique, deux lectures peuvent en être faites: celle d'une condamnation de l'insuffisance des garanties prévues par la directive; celle d'une condamnation de tout système de conservation générale des métadonnées, quel qu'il soit.

[…]

La première interprétation de cet arrêt peut se fonder sur le fait que la Cour a fait masse de trois éléments pour juger que le principe de proportionnalité était méconnu, et que le second avait trait à l'absence de toute précision sur les conditions d'accès des États aux métadonnées conservées par les opérateurs.

Selon cette interprétation, si la directive avait fixé des garanties concernant l'accès, l'appréciation de la Cour aurait peut-être été différente. Elle aurait également pu être influencée par l'existence de restrictions concernant la conservation, par exemple une durée maximale plus courte que celle de

deux ans fixée par la directive. Les conclusions de l'avocat général peuvent conforter une telle interprétation. L'avocat général déplorait le fait que la directive n'ait défini ni la nature des infractions pouvant justifier l'accès aux métadonnées, ni les autorités pouvant obtenir cet accès, ni les garanties relatives à l'effacement des données par les autorités après leur utilisation et à l'information des personnes concernées (§ 125 à 129 des conclusions). Il relevait aussi qu'il y avait une différence entre une durée de conservation se mesurant en mois et une durée se mesurant en années (§ 148). Cependant, si la Cour est parvenue à la même solution que l'avocat général, la construction de son raisonnement est assez différente, et il n'est donc pas évident que les conclusions permettent d'éclairer la portée de l'arrêt sur la condamnation du système de conservation en tant que tel.

La seconde interprétation se fonde en premier lieu sur ce que deux des trois éléments pris en compte par la Cour pour juger que le principe de proportionnalité est méconnu tiennent au caractère général et indiscriminé de la conservation: dans le premier élément, la Cour critique le fait que les métadonnées de tous les utilisateurs des communications soient collectées, indépendamment de l'existence d'un soupçon quant à la participation à une infraction grave; dans le troisième élément, c'est le fait que la durée de conservation soit fixée de manière indiscriminée qui est contesté. C'est donc le caractère systématique et uniformément durable de la conservation des métadonnées qui est en cause. En second lieu, l'arrêt qualifie sévèrement la conservation systématique des métadonnées, en y voyant une "ingérence particulièrement grave" dans les droits garantis par les articles 7 et 8 de la Charte, l'absence d'information des intéressés étant en outre "susceptible de générer dans l'esprit des personnes concernées (...) le sentiment que leur vie privée fait l'objet d'une surveillance constante". Si la Cour admet que la conservation préventive des données poursuit un but d'intérêt général, elle juge que l'ingérence ne peut être admise que si elle est proportionnée.

À l'issue de son contrôle de proportionnalité, elle conclut que la directive "comporte une ingérence dans des droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire" (§ 65). On peut donc en déduire que l'ingérence résultant d'un système de conservation systématique peut difficilement être considérée comme limitée au strict nécessaire".[9]

Dat het moeilijk is om een duidelijke draagwijdte te kennen aan het arrest van het Hof van Justitie en het feit dat een van de mogelijke interpretaties van dit arrest afbreuk doet aan het beginsel zelf van de verplichting om *a priori*-gegevens te bewaren zijn trouwens als volgt aan bod gekomen in de rechtsleer:

"[…] il est difficile de voir quelle garantie pourrait être prévue pour répondre à ce défaut de l'instrument sans changer fondamentalement le principe même de la conservation *a priori*

[9] *"Les rapports du Conseil d'État – Le numérique et les droits fondamentaux",* bron: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf, 198-201.

deux ans fixée par la directive. Les conclusions de l'avocat général peuvent conforter une telle interprétation. L'avocat général déplorait le fait que la directive n'ait défini ni la nature des infractions pouvant justifier l'accès aux métadonnées, ni les autorités pouvant obtenir cet accès, ni les garanties relatives à l'effacement des données par les autorités après leur utilisation et à l'information des personnes concernées (§ 125 à 129 des conclusions). Il relevait aussi qu'il y avait une différence entre une durée de conservation se mesurant en mois et une durée se mesurant en années (§ 148). Cependant, si la Cour est parvenue à la même solution que l'avocat général, la construction de son raisonnement est assez différente, et il n'est donc pas évident que les conclusions permettent d'éclairer la portée de l'arrêt sur la condamnation du système de conservation en tant que tel.

La seconde interprétation se fonde en premier lieu sur ce que deux des trois éléments pris en compte par la Cour pour juger que le principe de proportionnalité est méconnu tiennent au caractère général et indiscriminé de la conservation: dans le premier élément, la Cour critique le fait que les métadonnées de tous les utilisateurs des communications soient collectées, indépendamment de l'existence d'un soupçon quant à la participation à une infraction grave; dans le troisième élément, c'est le fait que la durée de conservation soit fixée de manière indiscriminée qui est contesté. C'est donc le caractère systématique et uniformément durable de la conservation des métadonnées qui est en cause. En second lieu, l'arrêt qualifie sévèrement la conservation systématique des métadonnées, en y voyant une "ingérence particulièrement grave" dans les droits garantis par les articles 7 et 8 de la Charte, l'absence d'information des intéressés étant en outre "susceptible de générer dans l'esprit des personnes concernées (...) le sentiment que leur vie privée fait l'objet d'une surveillance constante". Si la Cour admet que la conservation préventive des données poursuit un but d'intérêt général, elle juge que l'ingérence ne peut être admise que si elle est proportionnée.

À l'issue de son contrôle de proportionnalité, elle conclut que la directive "comporte une ingérence dans des droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire" (§ 65). On peut donc en déduire que l'ingérence résultant d'un système de conservation systématique peut difficilement être considérée comme limitée au strict nécessaire"[9].

Cette difficulté de conférer une portée certaine à l'arrêt de la Cour de justice et la circonstance qu'une des interprétations possibles de cet arrêt amène à mettre à mal le principe même de l'obligation de conservation des données *a priori*, ont été par ailleurs mises en exergue par la doctrine, en ces termes:

"[…] il est difficile de voir quelle garantie pourrait être prévue pour répondre à ce défaut de l'instrument sans changer fondamentalement le principe même de la conservation *a*

[9] *"Les rapports du Conseil d'État – Le numérique et les droits fondamentaux",* source: *http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf*, pp. 198 à 201.

contenu dans la directive. Cette partie du raisonnement de la Cour laisse donc perplexe: d'un côté, la Cour semble insister sur le fait que l'important est d'apporter des garanties compensatoires mais en même temps une des "garanties" à apporter remet en cause le principe même contenu dans la directive.

La Cour ne facilite donc pas l'intervention du législateur européen[10] pour "réparer" la directive 2006/24/CE: faut-il changer complètement d'approche voire abroger purement et simplement la directive (mais alors pourquoi la Cour ne l'a-t-elle pas clairement exprimé) ou cette critique adressée à la directive rend-elle seulement les autres garanties évoquées par la Cour d'autant plus importantes?

Ces questions rendent le sort du dossier très incertain".[11]

3.1.4. De steller van het voorontwerp heeft voor de eerste van de twee hierboven vermelde interpretaties gekozen en heeft in dat verband tegelijk gepoogd in vergelijking met de opgeheven wet[12] strengere vereisten en voorwaarden te verbinden aan de ingevoerde regeling wat betreft de garantie van vertrouwelijkheid en beveiliging van de gegevensbewaring, de procedure en de termijn gedurende welke de gegevens toegankelijk zijn, de bedoeling van deze toegang tot de gegevens en de overheden die gemachtigd zijn om toegang te hebben tot de gegevens alsook wat betreft de vernietiging van de gegevens zodra de bewaartermijn verstreken is, en daarbij schrijft hij bijzondere beschermingsmaatregelen voor met betrekking tot de gegevens die verband houden met de uitoefening van bepaalde beroepen die onder het beroepsgeheim vallen.[13]

10 De Europese Commissie heeft tot op heden geen enkel officieel initiatief genomen dat strekt tot opheffing of wijziging van richtlijn 2006/24/EG.

11 S. De Biolley en A. Weyembergh, "Chronique de jurisprudence consacrée à l'espace de liberté, de sécurité et de justice II – Jurisprudence de la Cour de justice relative à la coopération policière et judiciaire en matière pénale (2009-2014)" in *Cahiers de droit européen,* 50e jaargang (2014), nr. 2*,* 430-434. Zie ook P.-Y. Dethy, noot onder HvJEU 8 april 2014, C-293/12, *Digital Rights Ireland Ltd* en C-594/12, *Kärntner Landesregierung e.a.*, "Quelques réflexions sur l'arrêt C-293/12 et C-594/12", *Revue du droit des industries de réseau*, 2014/3, 338-349.

12 De steller van het voorontwerp sluit zich aldus aan bij de aanbevelingen van de Raad van State van Frankrijk die het volgende stelt: "L'arrêt de la C.J.U.E. soulève la question de la conformité au droit de l'Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion. Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l'étude du Conseil d'État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l'accès et l'utilisation de ces données." *("Les rapports du Conseil d'État – Le numérique et les droits fondamentaux",* bron: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf, 20).

13 In de hiernavolgende opmerkingen wordt elke maatregel onderzocht die in aanmerking wordt genomen voor die uitbreiding van de garanties; er wordt aangegeven wegens welke aspecten die maatregelen als ontoereikend zouden kunnen worden beschouwd in het licht van de rechtspraak van het Hof van Justitie en van het Grondwettelijk Hof en waar mogelijk worden verbeteringen voorgesteld, uiteraard binnen de grenzen van de wettigheidstoetsing die overeenkomstig de wet door de afdeling Wetgeving is verricht.

priori contenu dans la directive. Cette partie du raisonnement de la Cour laisse donc perplexe: d'un côté, la Cour semble insister sur le fait que l'important est d'apporter des garanties compensatoires mais en même temps une des "garanties" à apporter remet en cause le principe même contenu dans la directive.

La Cour ne facilite donc pas l'intervention du législateur européen[10] pour "réparer" la directive 2006/24/CE: faut-il changer complètement d'approche voire abroger purement et simplement la directive (mais alors pourquoi la Cour ne l'a-t-elle pas clairement exprimé) ou cette critique adressée à la directive rend-elle seulement les autres garanties évoquées par la Cour d'autant plus importantes?

Ces questions rendent le sort du dossier très incertain"[11].

3.1.4. L'auteur de l'avant-projet a retenu la première des deux interprétations mentionnées ci-avant, tout en s'efforçant, dans ce cadre, de renforcer par rapport à la loi annulée[12] les exigences et conditions attachées au système mis en place en termes de garantie de la confidentialité et de la sécurisation de la conservation des données, de procédure et de délai d'accès aux données, de finalité d'accès et d'autorités habilitées à accéder aux données ainsi qu'en termes de destruction des données une fois le délai de conservation expiré, et ce tout en envisageant des mesures de protection particulières pour les données en relation avec l'exercice de certaines professions soumises au secret professionnel[13].

10 À ce jour, la Commission européenne n'a pris d'initiative officielle relative à l'abrogation ou la modification de la directive 2006/24/CE.

11 S. De Biolley et A. Weyembergh, "Chronique de jurisprudence consacrée à l'espace de liberté, de sécurité et de justice II – Jurisprudence de la Cour de justice relative à la coopération policière et judiciaire en matière pénale (2009-2014)" in *Cahiers de droit européen,* 50e année (2014), n° 2*,* pp. 430 à 434. Voir également, P.-Y. Dethy, note sous C.J.U.E, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd* et C-594/12, *Kärntner Landesregierung e.a.*), *"Quelques réflexions sur l'arrêt C-293/12 et C-594/12"*, in *Revue du droit des industries de réseau*, 2014/3, pp. 338 à 349.

12 L'auteur de l'avant-projet se situe ainsi dans la ligne des recommandations du Conseil d'État de France, qui expose: "L'arrêt de la C.J.U.E. soulève la question de la conformité au droit de l'Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion. Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l'étude du Conseil d'État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l'accès et l'utilisation de ces données." (*"Les rapports du Conseil d'État – Le numérique et les droits fondamentaux",* source: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf, p. 20).

13 Les observations qui suivent examinent chacune des mesures envisagées pour assurer ce renforcement des garanties; elles indiquent les aspects pour lesquels ces mesures pourraient ne pas être qualifiées de suffisantes au regard de la jurisprudence de la Cour de justice et de la Cour constitutionnelle et proposent des améliorations, là où cela s'avère possible et, bien évidemment, dans les limites du contrôle de légalité effectué en vertu de la loi par la section de législation.

Tot staving van die soepeler interpretatie kan voornamelijk in aanmerking worden genomen dat het Hof van Justitie in zijn arrest het beginsel van de *a priori*-bewaring van gegevens niet uitdrukkelijk veroordeeld heeft, aangezien het heeft vastgesteld dat dit beginsel geen afbreuk deed aan de wezenlijke inhoud van de fundamentele vrijheden die in het geding zijn en tegemoetkomt aan een doelstelling van algemeen belang, namelijk de bescherming van de openbare veiligheid.[14]

De veroordeling van de *a priori*-bewaring van gegevens op zich, als daarbij geen onderscheid zou worden gemaakt wat betreft de onderscheiden wijzen waarop wordt gecommuniceerd en wat betreft de omstandigheden en de personen in kwestie, blijkt niet uit de latere rechtspraak van het Hof van Justitie. In die zin blijkt uit het arrest-*Schrems* van 6 oktober 2015[15] dat er alleen strijdigheid is met het recht van de Europese Unie, wanneer die veralgemeende gegevensbewaring gepaard gaat met de omstandigheid dat er geen objectief criterium bestaat voor de toegang van de overheden tot de aldus bewaarde gegevens en voor het gebruik ervan:

"Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens [zie in die zin, aangaande 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 elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (Pb.L. 105, 54), arrest Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 57-61]."

De afdeling Wetgeving stelt ten slotte dat tussen twee mogelijke interpretaties van de arresten van het Hof van Justitie en van het Grondwettelijk Hof in het licht van de rechtsregels die door beide hoven worden gehanteerd, gekozen moet worden voor de interpretatie waardoor de tegenstrijdige vereisten van het recht op eerbiediging van het privéleven van personen die gebruikmaken van elektronische communicatiemiddelen enerzijds en van de bescherming van personen die worden bedreigd door criminele praktijken van een ander anderzijds het best verzoend kunnen worden. De afdeling Wetgeving wijst er in dit verband op dat bij artikel 2 van het Europees Verdrag tot bescherming van de rechten van de mens aan

[14] Zie de punten 39, 42 en 44 van het arrest C-293/12 van het Hof van Justitie van de Europese Unie, *Digital Rights Ireland Ltd*, 8 april 2014.

[15] Zie HvJEU C-362/14, *Maximillian Schrems v. Data Protection commissioner*, 6 oktober 2015, punt 93.

À l'appui de cette interprétation plus souple, l'on peut essentiellement retenir que dans son arrêt, la Cour de justice n'a pas condamné expressément le principe de la conservation *a priori* des données constatant que celui-ci ne portait pas atteinte au contenu essentiel des libertés fondamentales en cause et qu'il répond à un objectif d'intérêt général, à savoir la protection de la sécurité publique[14].

La condamnation de la conservation *a priori* des données elle-même, fut-elle opérée de manière indifférenciée quant aux modes de communication visés et aux circonstances et personnes concernées, ne ressort pas davantage de la jurisprudence ultérieure de la Cour de Justice. L'arrêt *Schrems* du 6 octobre 2015[15] laisse en ce sens apparaître que la contrariété au droit de l'Union ne survient que lorsque cette conservation généralisée est couplée à l'absence de critère objectif encadrant l'accès des autorités aux données ainsi conservées et leur utilisation:

"Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données [voir en ce sens, en ce qui concerne la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54), arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 57 à 61]".

Enfin, la section de législation estime que, entre deux interprétations possibles des arrêts de la Cour de Justice et de la Cour constitutionnelle ainsi que des normes appliquées par l'une et l'autre, il y a lieu de retenir celle qui permet de concilier au mieux les impératifs contradictoires du droit au respect de la vie privée des personnes faisant usage des moyens de communications électroniques, d'un côté, et de la protection due aux droits des personnes menacées par les agissements criminels d'autrui, d'un autre côté. La section de législation rappelle en ce sens que l'article 2 de la Convention européenne des droits de l'Homme met à charge des autorités l'obligation de protéger la vie des personnes contre de

[14] Voir les paragraphes 39, 42 et 44 de l'arrêt C.J.U.E., n° C-293/12, 8 avril 2014 (Digital Rights Ireland Ltd).

[15] Voir C.J.U.E., n° C-362/14, 6 octobre 2015 (Maximillian Schrems c. Data Protection commissioner), pt. 93.

de overheden de verplichting wordt opgelegd het leven van personen te beschermen tegen dergelijke praktijken,[16] inzonderheid wanneer die de vorm aannemen van terrorisme.[17] Artikel 8 van hetzelfde verdrag, zijnerzijds, legt onder meer de verplichting op om de seksuele integriteit van kinderen inzonderheid in relaties naar behoren te beschermen en om te voorzien in een effectieve strafbaarstelling als die integriteit wordt aangetast, terwijl de anonimiteit die de internetgebruikers gegarandeerd wordt daaraan niet in de weg mag staan. In het arrest *K.U. v. Finland* van 2 december 2008, waarin uitspraak wordt gedaan over de bescherming van een kind dat nadeel had ondervonden van een seksueel getinte advertentie die op zijn naam gepubliceerd was op een datingsite, wordt (in punt 49) het volgende gesteld:

"Une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier et poursuivre l'auteur, c'est-à-dire la personne qui avait passé l'annonce. Or pareilles mesures n'ont pas été prises. La prépondérance ayant été accordée à l'exigence de confidentialité, il n'a jamais été possible de procéder à une enquête efficace. Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Sans préjudice de la question de savoir si, compte tenu de sa nature répréhensible, la conduite de la personne ayant passé l'annonce illégale sur Internet relève ou non de la protection des articles 8 et 10, le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte".

Niettemin zal de vraag over de werkelijke draagwijdte van arrest C-293/12, *Digital Rights Ireland Ltd* maar kunnen worden beantwoord in de toekomstige rechtspraak van het

[16] Zie EHRM, *Van Colle v. United Kingdom*, 13 november 2012.

[17] Zie EHRM, beslissing *Finogenov and Others v. Russia*, 18 maart 2010, verzoekschrift 18299/03.

tels agissements[16], notamment lorsqu'ils prennent la forme du terrorisme[17]. Quant à l'article 8 du même instrument, il impose entre autres que l'intégrité sexuelle des enfants soit adéquatement protégée dans les rapports en particulier et que les atteintes portées à cette intégrité donnent lieu à une répression pénale effective, sans que l'anonymat garanti aux utilisateurs de l'internet ne puisse y faire obstacle. Statuant à propos de la protection due à un enfant victime d'une annonce à caractère sexuel publiée à son nom sur un site de rencontre, un arrêt *K.U. c. Finlande* du 2 décembre 2008 énonce ce qui suit (§ 49):

"Une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier et poursuivre l'auteur, c'est-à-dire la personne qui avait passé l'annonce. Or pareilles mesures n'ont pas été prises. La prépondérance ayant été accordée à l'exigence de confidentialité, il n'a jamais été possible de procéder à une enquête efficace. Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Sans préjudice de la question de savoir si, compte tenu de sa nature répréhensible, la conduite de la personne ayant passé l'annonce illégale sur Internet relève ou non de la protection des articles 8 et 10, le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte".

Il reste que la question de la portée effective de l'arrêt C-293/12, *Digital Rights Ireland Ltd* ne pourra trouver une réponse que dans la jurisprudence future de la Cour de justice,

[16] Voir Cour eur. D.H., arrêt Van Colle c. Royaume-Uni, 13 novembre 2012.

[17] Voir Cour eur. D.H., déc. Finogenov and Others v. Russia, 18 mars 2010, req. n° 18299/03.

Hof van Justitie, wanneer dit Hof, zoals reeds het geval is,[18] uitspraak zal moeten doen over de wetgeving ter zake van de verschillende lidstaten, inzonderheid in het licht van artikel 15, lid 1, van de richtlijn 2002/58/EG en van de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie.

3.2. De vraag of de ontworpen tekst objectieve criteria vaststelt om de toegang van de bevoegde overheden tot de gegevens en het gebruik van die gegevens overeenkomstig de nagestreefde doelstellingen af te bakenen, inzonderheid wat de procedure betreft

3.2.1. In eerste instantie dient erop te worden gewezen dat richtlijn 2006/24/EG geen enkele bepaling bevatte waarbij de toegang tot de gegevens door de overheden van de lidstaten rechtstreeks werd geregeld. Aldus werd in artikel 4 van de richtlijn alleen het volgende bepaald:

"De lidstaten nemen bepalingen aan om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde nationale autoriteiten worden verstrekt. De procedure en de te vervullen voorwaarden voor toegang tot gegevens die bewaard worden overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid, worden door elke lidstaat vastgesteld in de nationale wetgeving, rekening houdend met de relevante bepalingen van de wetgeving van de Europese Unie of publiek internationaal recht, met name het EVRM, zoals geïnterpreteerd door het Europees Hof voor de Rechten van de Mens."

De wet van 30 juli 2013 die door het Grondwettelijk Hof is vernietigd, somde alleen de doeleinden van de bewaring op, zonder dat nauwkeurig was vastgesteld welke autoriteiten gemachtigd waren te vragen om toegang te krijgen tot de bewaarde gegevens of welke procedure daartoe moest worden gevolgd. Artikel 126, § 2, van de wet van 13 juni 2005, zoals ingevoegd bij de wet van 30 juli 2013, luidde immers als volgt:

lorsqu'elle sera appelée, comme c'est déjà le cas[18], à se prononcer sur les législations des différents États membres en la matière, spécialement au regard de l'article 15, paragraphe 1er, de la directive 2002/58/CE, et des articles 7, 8 et 52, de la Charte des droits fondamentaux de l'Union européenne.

3.2. Quant à la question de savoir si le texte en projet fixe des critères objectifs pour délimiter l'accès des autorités compétentes aux données et leur utilisation conformes aux objectifs poursuivis, en termes notamment de procédure

3.2.1. Dans un premier temps, il convient de rappeler que la directive 2006/24/CE ne comportait aucune disposition régissant directement l'accès aux données par les autorités des États membres. Ainsi, en son article 4, elle se bornait à prévoir que

"Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme".

Quant à la loi du 30 juillet 2013 annulée par la Cour constitutionnelle, elle énumérait seulement les finalités de la conservation, sans déterminer précisément les autorités habilitées à demander l'accès aux données conservées, ni la procédure à suivre. L'article 126, § 2, de la loi du 13 juin 2005, tel qu'inséré par la loi du 30 juillet 2013 prévoyait en effet que:

---

[18] Zie in dit verband het verzoek om een prejudiciële beslissing ingediend door Kammarrätten i Stockholm (Zweden) op 4 mei 2015 – Tele2 Sverige AB/Post- och telestyrelsen (Zaak C-203/15) (*Pb.C.* 2015, afl. 221/06), waarin door het Zweedse gerecht de volgende prejuciële vragen worden gesteld:
"1) Is een algemene verplichting (zoals beschreven [in het verzoek om een prejudiciële beslissing]), om met het oog op wetshandhaving op strafrechtelijk gebied verkeersgegevens te bewaren, welke verplichting zich zonder enig onderscheid, enige beperking of uitzondering uitstrekt tot alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, verenigbaar met artikel 15, lid 1, van richtlijn 2002/58EG(1), gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest van de Grondrechten van de Europese Unie?
2) Indien de eerste vraag ontkennend wordt beantwoord, kan de bewaring dan niettemin toegestaan zijn
a) wanneer de toegang van de nationale instanties tot de gegevens die worden bewaard, is geregeld zoals [beschreven in het verzoek om een prejudiciële beslissing],
b) wanneer de veiligheidseisen worden geregeld zoals [beschreven in het verzoek om een prejudiciële beslissing], en
c) alle relevante gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd, en daarna moeten worden gewist, zoals [beschreven in het verzoek om een prejudiciële beslissing]?".

[18] Voir à ce propos la demande de décision préjudicielle présentée par la Kammarrätten i Stockholm (Suède) le 4 mai 2015 – Tele2 Sverige AB/Post- och telestyrelsen (Affaire C-203/15) (*Journal officiel* 2015/C 221/06), dans laquelle la juridiction suédoise pose les questions préjudicielles suivantes:
"1) Une obligation générale de conservation de données, relative à toute personne et à tous les moyens de communication électronique et portant sur l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre la criminalité [telle que décrite dans la décision de renvoi], est-elle compatible avec l'article 15, paragraphe 1, de la directive 2002/58 (1) compte tenu des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne?
2) S'il est répondu par la négative à la première question, une telle obligation de conservation peut-elle néanmoins être admise:
a) si l'accès par les autorités nationales aux données conservées est encadré de la manière précisée [dans la décision de renvoi], et
b) si les exigences de protection et de sécurité des données sont régies de la manière précisée [dans la décision de renvoi], et que
c) toutes les données en question doivent être conservées pendant six mois à compter du jour de l'achèvement de la communication avant d'être effacées, comme il l'est exposé [dans la décision de renvoi]?".

"§ 2. De gegevens bedoeld in paragraaf 1, eerste lid, worden bewaard met het oog op:

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of –dienst, zoals bedoeld in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van 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.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten *a)* tot *d)* kunnen worden meegedeeld en uitsluitend aan deze laatsten."[19]

3.2.2. De ontworpen tekst strekt ertoe te bepalen welke autoriteiten of instanties gemachtigd zijn te vragen om toegang te krijgen tot de bewaarde gegevens, welke de doeleinden van deze toegang zijn en, afhankelijk van het doeleinde en van degene die om toegang vraagt, voor welke periode in het verleden deze autoriteiten of instanties toegang kunnen vragen. In bepaalde gevallen, zoals wanneer een nooddienst wordt opgeroepen of men de identiteit wil achterhalen van degene van wie een kwaadwillige oproep uitgaat, worden in de ontworpen tekst ook termijnen, te rekenen vanaf een welbepaald feit, bepaald waarbinnen de aanvragen bij de operator of aanbieder moeten worden ingediend.

[19] In artikel 126, § 5, 3°, dat bij de vernietigde wet in de wet van 13 juni 2005 werd ingevoegd, werd voorts bepaald dat de aanbieders in kwestie moesten "garande[ren] dat de toegang tot de bewaarde gegevens enkel gebeurt door een of meer leden van de Coördinatiecel Justitie bedoeld in 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 en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn". In tegenstelling tot wat uit het arrest van het Grondwettelijk Hof (B.10.3) zou kunnen worden afgeleid, werden daarmee niet de bevoegde "autoriteiten" bedoeld die gemachtigd zijn om tot de bewaarde gegevens toegang te hebben, maar wel de personeelsleden van de operator of aanbieder in kwestie, die gemachtigd worden toegang te hebben tot de gegevens om ze aan de autoriteit te kunnen overzenden, aangezien die bepaling niet moest zorgen voor de omzetting van artikel 4, maar wel van artikel 7, c), van richtlijn 2006/24/EG.

"§ 2. Les données visées au paragraphe 1er, alinéa 1er, sont conservées en vue:

a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle;

b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

d) de l'accomplissement 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.

Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er, soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières"[19].

3.2.2. Le texte en projet entend déterminer les autorités ou instances habilitées à demander l'accès aux données conservées, ainsi que les finalités de cet accès et, selon la finalité et le demandeur d'accès, la période temporelle du passé pour laquelle ces autorités ou instances peuvent demander l'accès. Dans certains cas, comme les hypothèses de l'appel à un service d'urgence ou l'identification de l'auteur d'un appel malveillant, le texte en projet fixe également des délais dans lesquels les demandes doivent être adressées à l'opérateur ou au fournisseur à dater d'un fait déterminé.

[19] La loi annulée prévoyait également en l'article 126, § 5, 3°, qu'elle insérait dans la loi du 13 juin 2005 que les fournisseurs concernés devaient "garanti[r] que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à 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 et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule". Contrairement à ce que pourrait laisser penser l'arrêt de la Cour constitutionnelle (B.10.3), étaient ainsi visées non pas les "autorités" compétentes habilitées à accéder aux données conservées, mais les membres du personnel de l'opérateur ou du fournisseur concerné, autorisés à avoir accès aux données en vue de les transmettre à l'autorité, cette disposition étant destinée à assurer la transposition non pas de l'article 4 de la directive 2006/24/CE, mais de l'article 7, c) de celle-ci.

3.2.2.1. Met betrekking tot de doelstellingen die erin bestaan actie te ondernemen om gevolg te geven aan een oproep naar een nooddienst of een vermiste persoon op te sporen wiens fysieke integriteit in onmiddellijk gevaar is, lijkt de inmenging in de uitoefening van fundamentele vrijheden minder ver te gaan dan in het kader van een optreden van de rechterlijke macht of de inlichtingen- en veiligheidsdiensten teneinde, naargelang het geval, inbreuken te voorkomen en te bestraffen of in het geheim inlichtingen in te winnen. Hetzelfde geldt wanneer een officier van gerechtelijke politie van het Instituut toegang vraagt met het oog op het opsporen, onderzoeken en vervolgen van schendingen van de artikelen 114 en 124 en het ontworpen artikel 126 van de wet van 13 juni 2005, aangezien het doeleinde er dan juist in bestaat te waarborgen dat de operatoren en de aanbieders de desbetreffende bepalingen naleven en dat zodoende de fundamentele rechten van de gebruikers in acht worden genomen.

In verband met de procedures voor de voornoemde aanvragen om toegang te krijgen, waarop de lering van het arrest van het Hof van Justitie om de hiervoor genoemde redenen *a priori* geen toepassing vindt, lijkt het niet overdreven om niet te voorzien in het voorafgaande optreden van een rechterlijke instantie of een administratieve overheid die waarborgen biedt inzake autonomie en onafhankelijkheid ten opzichte van de aanvrager van de toegang.

Dit neemt evenwel niet weg dat de procedurele waarborgen waarin de ontworpen tekst voorziet, niet toereikend blijken te zijn. In dat verband wordt verwezen naar de bijzondere opmerkingen die hierna worden gemaakt over artikel 3 van het voorontwerp (ontworpen artikel 126).

3.2.2.2. Hoewel de vraag die uitgaat van de Ombudsdienst voor Telecommunicatie volgens de ontworpen tekst alleen betrekking mag hebben op de identificatiegegevens, kan ze worden beschouwd als een meer ingrijpende aantasting van de rechten en vrijheden van de oproeper van wie de identificatie wordt gevraagd, aangezien artikel 43*bis*, § 3, eerste lid, 7°, van de wet van 21 maart 1991 “betreffende de hervorming van sommige economische overheidsbedrijven” aan de ombudsdienst de opdracht toevertrouwt om “van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische-communicatienetwerk of –dienst, het verzoek [te] onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische-communicatienetwerken of -diensten die

3.2.2.1. En ce qui concerne les finalités qui consistent à intervenir en vue de faire suite à un appel aux services d’urgence ou à rechercher une personne disparue dont l’intégrité physique est en danger imminent, l’ingérence dans l’exercice de libertés fondamentales apparaît moins importante que dans le cadre d’une intervention du pouvoir judiciaire ou des services de renseignements et de sécurité, en vue, selon le cas, de la prévention et de la répression d’infractions ou de la collecte secrète d’informations. Il en va de même lorsque l’accès est demandé par un 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 126 en projet, de la loi du 13 juin 2005, dès lors que la finalité est alors précisément de garantir le respect des dispositions considérées par les opérateurs et fournisseurs et par conséquent, de garantir le respect des droits fondamentaux des utilisateurs.

Concernant les procédures régissant les demandes d’accès précités, et auxquels l’enseignement de l’arrêt de la Cour de justice n’a pas vocation, *a priori*, à s’appliquer pour les raisons évoquées plus haut, il n’apparait pas disproportionné de ne pas prévoir l’intervention préalable d’une juridiction ou d’une autorité administrative présentant des garanties d’autonomie et d’indépendance par rapport au demandeur d’accès.

Il reste toutefois que les garanties procédurales prévues par le texte en projet ne s’avèrent pas suffisantes. Il est, sur ce point, renvoyé aux observations particulières ci-après, relatives à l’article 3 de l’avant-projet (article 126 en projet).

3.2.2.2. En ce qui concerne la demande émanant du Service de médiation pour les télécommunications, même si, selon le texte en projet, une telle demande ne peut porter que sur les données d’identification, elle peut être considérée comme entraînant une atteinte plus importante aux droits et libertés de l’appelant dont l’identification est demandée dès lors que l’article 43*bis*, § 3, alinéa 1er, 7°, de la loi du 21 mars 1991 “portant réforme de certaines entreprises publiques économiques” confie au service de médiation la mission d’examiner la demande de “toute personne se prétendant victime d’une utilisation malveillante d’un réseau ou d’un service de communications électroniques visant à obtenir communication de l’identité et l’adresse des utilisateurs de réseaux ou de services de communications électroniques

deze persoon hebben lastiggevallen, voorzover die gegevens beschikbaar zijn."[20]

Voor de toegang tot de gegevens die aldus aan de ombudsdienst zou worden verleend, moeten in die context specifieke waarborgen gelden. Er wordt eveneens verwezen naar de bijzondere opmerkingen over artikel 3 van het voorontwerp (ontworpen artikel 126).

3.2.2.3. Voor het geval waarin de aanvraag door de gerechtelijke instanties wordt ingediend om strafbare feiten op te sporen, te onderzoeken en te vervolgen met het doel uitvoering te geven aan de maatregelen bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering, voorzien deze artikelen in een precieze procedure voor de aanvragen om toegang, op het gebied van de gegevens waartoe toegang kan worden verkregen, de motivering van de beslissing, de evenredigheid van de toegang ten aanzien van de eerbiediging van het privéleven en de subsidiariteit ten opzichte van andere onderzoeksverrichtingen, de toegangsvoorwaarden en het beroepsgeheim, hetgeen waarborgen oplevert die bij de artikelen 8 en 9 van het voorontwerp uitgebreid worden, inzonderheid door de termijn voor toegang tot de bewaarde gegevens te beperken.

Gelet op de lering die kan worden getrokken uit de arresten van het Hof van Justitie en van het Grondwettelijk Hof, moet de steller van het voorontwerp erop toezien dat de ernst van de strafbare feiten waarvoor de toegang wordt aangevraagd, beter wordt gerechtvaardigd. Op dat punt dient de steller van het voorontwerp na te gaan of het, uiteraard rekening houdend met de in acht te nemen doeleinden, niet beter zou zijn de lijst van de strafbare feiten waarvoor de toegang toegestaan

[20] Er dient op gewezen te worden dat het feit dat de aanvraag die van de ombudsdienst uitgaat, ertoe kan leiden dat de identiteit en het adres van de oproeper worden meegedeeld aan een particulier, en niet aan een autoriteit, voortvloeit uit het voornoemde artikel 43*bis,* welke bepaling bij het voorontwerp niet wordt gewijzigd en die, samen met andere wetsbepalingen die vervat zijn in de wet van 13 juni 2005, bijdraagt tot de omzetting van artikel 10 van richtlijn 2002/58/EG, waarin met name het volgende wordt bepaald:
"De lidstaten zorgen ervoor dat er transparante procedures zijn waarin is vastgelegd hoe de aanbieder van een openbaar communicatienetwerk en/of een openbare elektronischecommunicatiedienst de volgende dienstenelementen kan opheffen: (...) de uitschakeling van de weergave van de identificatie van het oproepende nummer op tijdelijke basis, op verzoek van een abonnee die kwaadwillige of hinderlijke oproepen wil traceren. In dat geval worden de identificatiegegevens van de oproepende abonnee overeenkomstig de nationale wetgeving opgeslagen en beschikbaar gesteld door de aanbieder van een openbaar communicatienetwerk en/of van een openbare elektronische-communicatiedienst;".

l'ayant importunée, pour autant que ces données sont disponibles"[20].

L'accès aux données qui serait ainsi octroyé au service de médiation doit, dans ce contexte, être entouré de garanties spécifiques. Il est également renvoyé aux observations particulières relatives à l'article 3 de l'avant-projet (article 126 en projet).

3.2.2.3. S'agissant de l'hypothèse où la demande émane des autorités judiciaires en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle, ces articles organisent une procédure précise concernant les demandes d'accès, en termes de données auxquelles il peut être accédé, de motivation de la décision, de proportionnalité de l'accès au regard du respect de la vie privée et de subsidiarité par rapport à d'autres devoirs d'enquête, de conditions d'accès et de secret professionnel, garanties qu'en ses articles 8 et 9, l'avant-projet envisage de renforcer, notamment en limitant le délai d'accès aux données conservées.

Au regard de l'enseignement des arrêts de la Cour de justice et de la Cour constitutionnelle, l'auteur de l'avant-projet doit veiller à mieux justifier le caractère de gravité des infractions pour lesquelles l'accès est demandé. Sur ce point, il convient que l'auteur de l'avant-projet vérifie s'il ne conviendrait pas, compte tenu bien évidemment des finalités à respecter, d'établir une liste plus restreinte des infractions pour lesquelles l'accès est autorisé, en énumérant plus

[20] Il convient de souligner que le fait que la demande émanant du service de médiation puisse avoir pour effet d'aboutir à la communication de l'identité et de l'adresse de l'appelant à un particulier, et non à une autorité, découle de l'article 43*bis* précité, disposition dont la modification n'est pas envisagée par l'auteur de l'avant-projet, et qui participe, avec d'autres dispositions législatives contenues dans la loi du 13 juin 2005 à la transposition de l'article 10 de la directive 2002/58/CE, lequel prévoit notamment que:
"Les États membres veillent à ce que des procédures transparentes régissent les modalités grâce auxquelles le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessible au public peut passer outre […] à la suppression de la présentation de l'identification de la ligne appelante, à titre temporaire, lorsqu'un abonné demande l'identification d'appels malveillants ou dérangeants; dans ce cas, conformément au droit interne, les données permettant d'identifier l'abonné appelant seront conservées et mises à disposition par le fournisseur d'un réseau public de communications et/ou d'un service de communications électroniques accessible au public;".

wordt, te beperken door van deze strafbare feiten een nauw keuriger opsomming te geven, zoals in artikel 90*ter* van het Wetboek van Strafvordering.[21]

Voor het overige wordt verwezen naar de bijzondere opmerkingen over de artikelen 8 en 9 van het voorontwerp.

3.3. Het feit dat de ontworpen tekst in het algemeen betrekking heeft op alle middelen voor elektronische communicatie en op alle gegevens betreffende het verkeer en het feit dat de ontworpen tekst niet voorziet in een bewaringstermijn waarbij tussen de categorieën van gegevens een onderscheid zou worden gemaakt op basis van hun eventuele nut voor de nagestreefde doelstelling of naargelang van de betrokken personen.

3.3.1. Hier rijst in de eerste plaats de vraag enerzijds te voorzien in een algemene verplichting om alle gegevens betreffende het verkeer voor alle middelen voor elektronische communicatie te bewaren en anderzijds niet te voorzien in verschillende bewaringstermijnen naargelang van de categorieën van gegevens ingedeeld op basis van hun nut, het evenredigheidsbeginsel eerbiedigen.

Zowel in het arrest van het Hof van Justitie als in het arrest van het Grondwettelijk Hof is er vóór elke andere opmerking op gewezen dat richtlijn 2006/24/EG en de Belgische wet op zeer algemene wijze betrekking hadden op alle verkeersgegevens betreffende vaste telefonie, mobiele telefonie, toegang tot internet, e-mail via internet en internettelefonie.

In antwoord op een vraag over de situatie op het vlak van gegevensbewaring in andere lidstaten van de Europese Unie, van welke situatie in de memorie van toelichting gewag wordt gemaakt en op welke situatie men zich wil baseren, heeft de gemachtigde van de minister aan de afdeling Wetgeving informatie bezorgd waaruit blijkt dat bepaalde lidstaten, die weliswaar een minderheid vormen, het plan hebben opgevat of overwegen om, naargelang van de aard van de gegevens, te voorzien in een verschillende aanpak op het gebied van verplichting tot en termijn van bewaring: zo zou in Duitsland de ontworpen bewaringstermijn variëren naargelang het gaat om verkeers- of om lokalisatiegegevens, waarbij voor de lokalisatiegegevens wordt voorzien in een kortere bewaringstermijn, met dien verstande dat gegevens betreffende de e-mails niet onder de bewaarplicht zouden vallen; in Nederland zou de ontworpen wetgeving voorzien in een bewaringstermijn van twaalf maanden voor telefoniegegevens en van zes maanden voor internetgegevens.

[21] Als een dergelijke lijst kan worden opgesteld, zal deze uitgebreider kunnen zijn dan de lijst die in artikel 90*ter* is opgenomen, aangezien dat artikel betrekking heeft op een meer ingrijpende inmenging in het privéleven en de gegevensbescherming, daar de onderzoeksrechter zich op grond van die bepaling toegang mag verschaffen tot de inhoud van privécommunicatie en –telecommunicatie, daarvan kennis kan nemen en ze kan opnemen: deze bepaling staat dus de toegang tot de inhoud toe, wat niet het geval is met de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering of met de ontworpen artikelen 126 en 126/1 van de wet van 13 juni 2005.

précisément celles-ci, à l'instar de l'article 90*ter* du Code d'instruction criminelle[21].

Pour le surplus, il est renvoyé aux observations particulières sous les articles 8 et 9 de l'avant-projet.

3.3. Quant au fait que le texte en projet porte généralement sur tous les moyens de communications électroniques ainsi que l'ensemble des données relatives au trafic et quant au fait que le texte en projet ne fixe pas une durée de conservation en opérant une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées

3.3.1. Se pose ici la question de la proportionnalité tout d'abord, d'une obligation générale de conserver toutes les données relatives au trafic pour tous les moyens de communications électroniques, et d'autre part, de l'absence de fixation de délais de conservation différents selon les catégories de données en fonction de leur utilité.

Tant l'arrêt de la Cour de Justice que celui de la Cour constitutionnelle ont, avant tout autre élément, relevé que la directive 2006/24/CE ou la loi belge concernait, de manière très générale, toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet.

Interrogé sur la situation en matière de conservation de données dans d'autres États membres de l'Union européenne, situation dont l'exposé des motifs fait état et sur laquelle il entend s'appuyer, le délégué du ministre a communiqué à la section de législation des informations dont il ressort que certains États membres, certes minoritaires, ont prévu ou envisagent d'adopter des traitements différenciés, en termes d'obligation et de durée de conservation, selon la nature des données: ainsi, en Allemagne, le délai de conservation en projet varierait selon qu'il s'agit de données de trafic ou de données de localisation, un délai plus bref étant prévu pour ces dernières, étant entendu que les données relatives aux e-mails seraient exclues de l'obligation de conservation; quant aux Pays-Bas, la législation en projet prévoirait un délai de conservation de douze mois pour les données relatives à la téléphonie, et de six mois, pour les données relatives à l'Internet.

[21] Si une telle liste peut être établie, elle pourra s'avérer plus large que celle qui figure à l'article 90*ter*, dès lors que ce dernier concerne une ingérence plus importante dans la vie privée et la protection des données puisqu'il permet au juge d'instruction d'accéder au contenu des communications et télécommunications privées, d'en prendre connaissance et de les enregistrer: cette disposition autorise donc un accès au contenu, ce qui n'est pas le cas des articles 46*bis* et 88*bis* du Code d'instruction criminelle ni des articles 126 et 126/1 en projet de la loi du 13 juin 2005.

Over deze kwesties wordt in de memorie van toelichting het volgende vermeld:

"Dit ontwerp van wet voert een onderscheid in op grond van drie categorieën van gegevens.

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, worden het meest gevraagd en tasten de persoonlijke levenssfeer op matige wijze aan, in vergelijking met inzonderheid de tweede en derde categorie.

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

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

De tweede en derde categorie tasten de persoonlijke levenssfeer meer aan dan de eerste. De toegangen tot die gegevens zijn minder talrijk dan die tot de identificatiegegevens maar blijven frequent.

Na veelvuldige besprekingen in de Regering en met de diensten en overheden in kwestie, en na een differentiatie in de bewaringstermijnen overwogen te hebben in functie van de categorieën van gegevens, is de conclusie dat, gelet op de noodwendigheden inzake de strijd tegen terroristische misdrijven, een bewaringsperiode van 12 maanden noodzakelijk is voor elk van de 3 categorieën."

3.3.2. Door af te stappen van het idee dat alle gegevens bewaard moeten worden of door de bewaringstermijn van de gegevens aan te passen naar gelang van de categorieën van gegevens, zou wellicht een regeling worden ingevoerd die betere waarborgen biedt om ervoor te zorgen dat de overwogen maatregelen, die een inmenging vormen in het recht op eerbiediging van het privéleven, conform aan het evenredigheidsbeginsel zijn.

Indien geopteerd zou worden voor een strikte uitlegging van de hiervoor in herinnering gebrachte vereisten, zou er dan ook van uit kunnen worden gegaan dat de ontworpen regeling blootstaat aan kritiek wegens de keuze die de steller van het voorontwerp gemaakt heeft.

In het licht van de onderscheiden doelstellingen die nagestreefd worden, en inzonderheid van de bestrijding van terrorisme en kinderpornografie, van de actie die ondernomen wordt naar aanleiding van een dringende oproep of van de opsporing van vermiste personen wier leven geacht wordt in onmiddellijk gevaar te zijn, dient evenwel te worden vastgesteld dat het de afdeling Wetgeving niet echt duidelijk is hoe die doelstellingen, die alle gerechtvaardigd zijn, efficiënt zouden kunnen worden gehaald als bijvoorbeeld zou worden bepaald dat alleen de telefoniegegevens en niet de internetgegevens moeten worden bewaard of door te voorzien in verschillende bewaringstermijnen voor bepaalde categorieën van gegevens. Bovendien stuit de invoering van een regeling waarbij, naargelang van het doel of de betrokken personen, een verschil in

Sur ces questions, l'exposé des motifs mentionne ce qui suit:

"Le présent projet de loi introduit une distinction sur base de 3 catégories de données.

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 sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux deuxième et troisième catégories.

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

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

Les deuxième et troisième catégories sont plus attentatoires à la vie privée que la première. Les accès à ces données sont moins nombreux que ceux aux données d'identification mais restent fréquents.

Après de nombreuses discussions au sein du gouvernement et avec les services et autorités concernées, et après avoir envisagé une différenciation entre les délais de conservation en fonction des catégories de données, la conclusion est que, vu les nécessités liées à la lutte contre les infractions terroristes, une période de 12 mois de conservation est nécessaire pour chacune des 3 catégories".

3.3.2. Restreindre la généralité des données à conserver, ou adapter le délai de conservation des données, selon les catégories de données, participerait sans doute d'un système de garanties plus importantes, en vue d'assurer la proportionnalité des mesures envisagées dans l'ingérence qu'elles constituent dans le droit au respect de la vie privée.

Aussi, si tant est que l'on retienne une lecture stricte des exigences rappelées ci-avant, le choix opéré par l'auteur de l'avant-projet pourrait apparaître comme fragilisant le système en projet.

Toutefois, il convient de constater qu'au regard des différentes finalités poursuivies, notamment la lutte contre le terrorisme et la pédopornographie, l'intervention faisant suite à un appel urgent, ou la recherche de personnes disparues dont la vie est estimée en danger imminent, la section de législation n'aperçoit pas, effectivement, comment ces finalités, toutes légitimes, pourraient être efficacement atteintes en imposant, par exemple, de conserver les seules données de téléphonie, et non les données internet, ou en prévoyant des délais de conservation différents pour certaines catégories de données. Par ailleurs, la mise en place d'un système dans lequel une différence de traitement est opérée en termes d'obligation même de conservation et de durée de celle-ci, selon la finalité ou les personnes concernées, se heurte

behandeling wordt ingevoerd op het stuk van de bewaarplicht zelf en van de duur ervan, voorts op dezelfde hinderpalen als die welke hiervoor in opmerking 3.1. zijn vermeld.

Om ervoor te zorgen dat overwogen maatregelen conform aan het evenredigheidsbeginsel zijn, voorziet de ontworpen tekst bovendien in verschillende toegangsregelingen qua toegangstermijn en qua gegevens waarvoor de toegang wordt verleend, naargelang van het doel zelf van de toegang of van de autoriteit die om toegang verzoekt. Zo zullen de hulpdiensten bijvoorbeeld alleen toegang hebben tot de identificatiegegevens van de oproeper[22], zal de toegang in het kader van de opsporing van een vermiste persoon alleen betrekking kunnen hebben op de gegevens met betrekking tot die persoon[23], en zijn de gegevens waartoe de procureur des Koning toegang kan hebben minder uitgebreid dan de gegevens waartoe de onderzoeksrechter toegang heeft[24]. De toegangstermijn, zijnerzijds, varieert van vierentwintig uur tot twaalf maanden, waarbij in de termijn van twaalf maanden wordt voorzien voor een gerechtelijke overheid die optreedt in het kader van haar actie met betrekking tot een strafbaar feit bedoeld in titel I*ter* van boek II van het Strafwetboek (te weten de terroristische misdrijven) en voor inlichtingen- en veiligheidsdiensten die optreden in het kader van een terroristische of extremistische bedreiging in de zin van de wet van 30 november 1998 “houdende regeling van de inlichtingen- en veiligheidsdienst”.

Bij de ontworpen regeling wordt dus een verschil in behandeling ingevoerd naargelang van het doel de toegang en van de aanvrager van de toegang, om een grotere evenredigheid te garanderen ten aanzien van het recht op eerbiediging van het privéleven.

3.4. Het feit dat de ontworpen tekst specifieke en aangepaste regels bevat die bedoeld zijn om de volle integriteit en vertrouwelijkheid van de gegevens te waarborgen en ervoor te zorgen dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd door een bijzonder hoog niveau van bescherming en beveiliging te bieden via technische en organisatorische maatregelen

3.4.1. De steller van het voorontwerp heeft aan deze dimensie bijzondere aandacht besteed, met dien verstande dat het beter waarborgen van de volle integriteit en vertrouwelijkheid van de gegevens volgens hem de omstandigheid zou kunnen compenseren dat de ontworpen tekst onmogelijk kan voldoen aan het eerste vereiste dat door het Hof van Justitie is geformuleerd, te weten dat een onderscheid zou moeten worden gemaakt qua categorie van gegevens en qua personen, alsook qua geografische zone en quaperiode.

De maatregelen die vervat zijn in de ontworpen tekst (ontworpen artikelen 126 en 126/1) en, in voorkomend geval, in andere geldende wet- of regelgeving, kunnen als volgt worden samengevat:

[22] Ontworpen artikel 126, § 2, eerste lid, 4°.
[23] Ontworpen artikel 126, § 2, eerste lid, 5°.
[24] Vergelijk de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering.

au demeurant aux mêmes obstacles que ceux évoqués à l’observation 3.1. ci-avant.

En outre, en vue d’assurer la proportionnalité des mesures envisagées, le texte en projet prévoit des accès différenciés en termes de données auxquelles l’accès est autorisé, et de délai d’accès, selon la finalité même de l’accès ou l’autorité qui demande l’accès. Ainsi, à titre d’exemple, les services d’urgence n’auront accès qu’aux données d’identification de l’appelant[22], l’accès dans le cadre d’une recherche de personne disparue ne pourra porter que sur les données relatives à cette personne[23], et le procureur du Roi accède à des données moins étendues que le juge d’instruction[24]. Quant au délai d’accès, celui-ci varie de vingt-quatre heures à douze mois, le délai de douze mois étant prévu lorsqu’une autorité judiciaire ou des services de renseignement et de sécurité agissent, pour la première dans le cadre de son action relative à une infraction visée au titre I*ter* du livre II du Code pénal (à savoir les infractions terroristes), et pour les seconds, de menace terroriste ou extrémiste au sens de la loi du 30 novembre 1998 “organique des services de renseignement et de sécurité”.

Le système en projet opère donc une différence de traitement selon la finalité de l’accès et le demandeur d’accès, de nature à tendre vers une plus grande proportionnalité du système au regard du droit au respect de la vie privée.

3.4. Quant au fait que le texte en projet comprenne des règles spécifiques et adaptées destinées à garantir la pleine intégrité et confidentialité des données ainsi que leur destruction irrémédiable au terme de leur durée de conservation, ce par un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles

3.4.1. L’auteur de l’avant-projet a été particulièrement attentif à cette dimension, étant entendu qu’une garantie accrue de la pleine intégrité des données et de la confidentialité de celles-ci serait, selon lui, de nature à compenser la circonstance que le texte en projet est dans l’impossibilité de faire suite à la première exigence formulée par la Cour de justice, à savoir, la non-généralité en termes de données et de personnes, ainsi que de zone géographique et de période temporelle.

Les mesures contenues par le texte en projet (articles 126 et 126/1 en projet), ainsi que, le cas échéant, par d’autres législations ou règlementations en vigueur peuvent être résumées comme suit.

[22] Article 126, § 2, alinéa 1er, 4°, en projet.
[23] Article 126, § 2, alinéa 1er, 5°, en projet.
[24] Comparez les articles 46*bis* et 88*bis* du Code d’instruction criminelle.

1° In de eerste plaats dient de algemene wet- en regelgeving inzake de bescherming van de persoonsgegevens en de verwerking ervan te worden toegepast. In dat verband wordt bepaald dat elke betrokken operator en aanbieder wordt beschouwd als verantwoordelijke 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 de persoonsgegevens" voor de gegevens die worden verwerkt op grond van de ontworpen artikelen 126 en 126/1.[25]

2° In principe wordt binnen elke betrokken operator of aanbieder een Coördinatiecel opgericht[26] die ermee belast is aan de wettelijk bevoegde Belgische autoriteiten op hun verzoek de bewaarde gegevens te verstrekken; toegang tot de gegevens kan alleen verleend worden aan de leden van de cel[27] die elk het voorwerp moeten hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies[28], conform artikel 22*quinquies* van de wet van 11 december 1998 "betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen"[29], en niet het voorwerp mogen hebben uitgemaakt van een weigering door de minister van Justitie, welke weigeringsbeslissing moet worden gemotiveerd en ten allen tijde kan worden genomen[30]; de leden van de cel mogen, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator of de aanbieder, met dien verstande dat zowel de leden van de cel als de aangestelden die aan hen technische bijstand verlenen, onderworpen zijn aan het beroepsgeheim[31]; de operatoren en aanbieders moeten waken over de vertrouwelijkheid van de gegevens die verwerkt worden door de cel en moeten zowel het BIPT als de Commissie voor de bescherming van de persoonlijke levenssfeer op de hoogte brengen van de contactgegevens van de cel en van haar leden en van de wijzigingen van die gegevens[32]; om ervoor te zorgen dat de gegevens daadwerkelijk vertrouwelijk verwerkt worden (waarbij tevens een beroepsgeheim geldt), wordt voorts voorzien in nieuwe strafbaarstellingen[33] die betrekking hebben op gedragingen die nog niet vallen onder artikel 550*bis* van het Strafwetboek, waarbij strafrechtelijke straffen worden gesteld op interne en externe hacking; wat de procedure betreft, zijn de operatoren en aanbieders verplicht om een interne procedure uit

25 Ontworpen artikel 126/1, § 2, tweede lid.
26 De operatoren en aanbieders kunnen ervoor kiezen een gemeenschappelijke Coördinatiecel op te richten die in dat geval moet voorzien in dezelfde dienst voor elke operator of aanbieder individueel (ontworpen 126/1, § 1, tweede lid).
27 Ontworpen artikel 126, § 4, 3°.
28 Het advies wordt vijf jaar na het verlenen ervan als vervallen beschouwd.
29 Ontworpen artikel 126/1, § 1, derde lid, 1°.
30 Ontworpen artikel 126/1, § 1, derde lid, 2°.
31 Ontworpen artikel 126/1, § 1, vijfde en zesde lid.
32 Ontworpen artikel 126/1, § 1, zevende lid.
33 Ontworpen artikel 145, § 3*ter.*

1° Il convient d'appliquer au premier chef la législation et la réglementation générales en matière de protection des données à caractère personnel et de traitement de celles-ci. Sur ce point, il est prévu que chaque opérateur et chaque fournisseur concerné 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 la base des articles 126 et 126/1 en projet[25].

2° Au sein de chaque opérateur ou fournisseur concerné est en principe créée une Cellule de coordination[26], chargée de fournir aux autorités belges légalement habilitées, à leur demande, les données conservées; l'accès aux données est réservé aux membres de la Cellule[27], lesquels doivent, chacun, avoir fait l'objet d'un avis de sécurité positif et non périmé[28] 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"[29] et ne pas avoir fait l'objet d'un refus du ministre de la Justice, refus qui doit être motivé et peut intervenir en tout temps[30]; les membres de la Cellule peuvent, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur ou du fournisseur, étant entendu que tant les membres de la cellule que les préposés qui leur apportent un soutien technique sont soumis au secret professionnel[31]; les opérateurs et fournisseurs doivent veiller à la confidentialité des données traitées par le Cellule et informer tant l'IBPT que la Commission pour la protection de la vie privée des coordonnées de la Cellule et de ses membres, ainsi que des modifications de ces données[32]; en outre, de nouvelles incriminations[33] sont prévues pour assurer l'effectivité de cette confidentialité (avec le secret professionnel par ailleurs imposé), incriminations qui couvrent des hypothèses non encore couvertes par l'article 550*bis* du Code pénal, lequel sanctionne pénalement les hackings interne et externe; s'agissant de la procédure, les opérateurs et fournisseurs sont tenus d'établir une procédure interne de réponse aux demandes d'accès des autorités aux données à caractère personnel des utilisateurs, et les informations relatives à ces procédures, au nombre de demandes reçues, à la base juridique invoquée et à la réponse, sont mises à la disposition de l'IBPT à sa

25 Article 126/1, § 2, alinéa 2, en projet.
26 Les opérateurs et les fournisseurs ont la possibilité de créer une Cellule commune, laquelle doit prévoir, dans ce cas, le même service pour chaque opérateur ou fournisseur individuel (article 126/1, § 1er, alinéa 2, en projet).
27 Article 126, § 4, 3°, en projet.
28 L'avis est considéré comme périmé cinq ans après son octroi.
29 Article 126/1, § 1er, alinéa 3, 1°, en projet.
30 Article 126/1, § 1er, alinéa 3, 2°, en projet.
31 Article 126/1, § 1er, alinéas 5 et 6, en projet.
32 Article 126/1, § 1er, alinéa 7, en projet.
33 Article 145, § 3*ter*, en projet.

te werken om te antwoorden op de verzoeken vanwege de autoriteiten om toegang te krijgen tot de persoonsgegevens van de gebruikers; de gegevens over deze procedures, over het aantal ontvangen verzoeken, over de aangevoerde rechtsgrond en over het antwoord worden op verzoek van het BIPT aan dat Instituut verstrekt[34]; bovendien moeten de operatoren van openbare netwerken en de betrokken aanbieders artikel 114, § 2, van de wet van 13 juni 2005 in acht nemen voor de toegang tot de bedoelde gegevens en het bezorgen ervan aan de autoriteiten[35]. Voorts wordt bepaald dat elke betrokken aanbieder en operator één of meer aangestelden voor de bescherming van persoonsgegevens moeten aanwijzen die moeten voldoen aan dezelfde voorwaarden als de leden van de Coördinatiecel; de aangestelden mogen in principe geen deel uitmaken van de cel en zij moeten in hun handelen onafhankelijk zijn, welke onafhankelijkheid inzonderheid wordt gewaarborgd door het feit dat de uitoefening van hun opdrachten voor hen geen nadelen met zich mag brengen en dat ze zonder grondige motivering niet mogen worden ontslagen of vervangen wegens de uitvoering van de taken die aan hen zijn toevertrouwd en dat ze de mogelijkheid moeten hebben om rechtstreeks te communiceren met het management of het directiecomité; deze aangestelden hebben tot taak ervoor te zorgen dat de verwerkingen door de Coördinatiecel conform de wet geschieden, dat de aanbieder of de operator alleen die gegevens verzamelt en bewaart die hij wettelijk mag bewaren, dat alleen de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens en dat de maatregelen voor beveiliging en bescherming van de persoonsgegevens die zijn beschreven in de wet en in het veiligheidsbeleid van de aanbieder of de operator, worden uitgevoerd tenslotte deelt elke betrokken aanbieder en operator 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[36].

3° Met betrekking tot de veeleer technische regels die de bewaring, de vertrouwelijkheid en de vernietiging van de

[34] Ontworpen artikel 126/1, § 2, eerste lid.

[35] Ontworpen artikel 126/1, § 2, derde lid. Artikel 114, § 2, van de wet van 13 juni 2005 luidt als volgt:
"Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, zorgen de in de eerste paragraaf bedoelde maatregelen die genomen worden door de ondernemingen die openbare elektronische-communicatiediensten aanbieden wanneer het persoonsgegevens betreft, ervoor dat in ieder geval:

— wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;
— opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en
— een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.
Het Instituut kan de door de aanbieders van openbare elektronische-communicatiediensten genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligings-peil dat met deze maatregelen moet worden gehaald."

[36] Ontworpen artikel 126/1, § 3.

demande[34]; de surcroît, les opérateurs de réseaux publics et les fournisseurs concernés respectent l'article 114, § 2, de la loi du 13 juin 2005 pour l'accès aux données visées et leur transmission aux autorités[35]. Il est également prévu que chaque fournisseur et opérateur concerné doit désigner un ou plusieurs préposés à la protection des données à caractère personnel, qui sont tenus de répondre aux mêmes conditions que les membres de la Cellule de coordination; les préposés ne peuvent pas faire partie, en principe, de la Cellule, et leur indépendance est prévue et garantie notamment par le fait que l'exercice de leur mission ne peut entraîner de désavantages pour eux, qu'ils ne peuvent être licenciés ou remplacés à cause de l'exécution des tâches qui leurs sont confiées sans motivation approfondie, et qu'ils doivent avoir la possibilité de communiquer directement avec le management ou le comité de direction; ces préposés ont pour mission de veiller à ce que les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi, à ce que le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver, à ce que seules les autorités légalement autorisées aient accès aux données conservées et à ce que les mesures de sécurité et de protection des données à caractère personnel décrites dans la loi et dans la politique de sécurité du fournisseur ou de l'opérateur soient mises en œuvre; enfin, chaque fournisseur et opérateur concerné 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[36].

3° S'agissant des règles de nature plus technique, destinées à garantir la conservation, la confidentialité et la

[34] Article 126/1, § 2, alinéa 1er, en projet.

[35] Article 126/1, § 2, alinéa 3, en projet. L'article 114, § 2, de la loi du 13 juin 2005 dispose comme suit:
"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 mesures prévues au paragraphe 1er que prennent les entreprises fournissant des services de communications électroniques accessibles au public, lorsqu'elles concernent des données à caractère personnel, visent pour le moins à:
— garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel;
— protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites; et
— assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.
L'Institut est habilité à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre".

[36] Article 126/1, § 3, en projet.

gegevens na afloop van de bewaringstermijn ervan moeten waarborgen, legt de de ontworpen tekst aan de operatoren en aanbieders de verplichting op te garanderen dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk, ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen onopzetelijke of onrechtmatige vernietiging, tegen onopzettelijk verlies of onopzettelijke wijziging, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, 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, en ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, zoals vastgelegd in het ontworpen artikel 126, § 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123 van de wet van 13 juni 2005; ten slotte moeten ze ervoor zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit die hiertoe is gemachtigd; deze opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek dat het BIPT en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen raadplegen of waarvan ze een volledige of gedeeltelijke kopie mogen eisen.[37]

3.4.2. Uit het voorgaande volgt dat met het ontwerp een bijzonder sterk uitgewerkte en alomvattende regeling wordt ingevoerd die zowel in rechte als in feite de volle integriteit en vertrouwelijkheid van de gegevens waarborgt en garandeert dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd welke regeling gekenmerkt wordt door "een bijzonder hoog niveau van bescherming en beveiliging" dat tot stand gebracht wordt door "technische en organisatorische maatregelen".[38]

Om volledig tegemoet te komen aan de vereisten waaraan volgens het arrest van het Hof van Justitie in dat verband moet worden voldaan, zou het ontwerp evenwel op enkele punten moeten worden herzien.

3.4.2.1. Uit het ontworpen artikel 126/1, § 1, vierde lid, blijkt dat de Koning gemachtigd is om bij een besluit vastgesteld na overleg in de Ministerraad bepaalde categorieën van operatoren en aanbieders vrij te stellen van de verplichting om te voldoen aan de vereisten die wat de leden van de Coördinatiecel betreft, worden gesteld in het derde lid van dezelfde paragraaf, in verband met het veiligheidsadvies en een niet-weigering van de minister van Justitie, of om voor die categorieën minder strikte voorwaarden vast te stellen.

In de bespreking van het artikel wordt daaromtrent het volgende gezegd:

"Er moet echter rekening worden gehouden met het feit dat afhankelijk van de evolutie van de actoren, het wetsontwerp van toepassing kan zijn op kleine aanbieders of operatoren, voor wie sommige van deze verificaties disproportioneel

[37] Ontworpen artikel 126, § 4.
[38] HvJ, C-293/12, *Digital Rights Ireland Ltd*, punt 67.

destruction des données au terme de leur délai de conservation, le texte en projet impose aux opérateurs et aux fournisseurs de garantir que les données conservées sont de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau, de veiller 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, de mettre 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 et de détruire les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé à l'article 126, § 3, en projet, sans préjudice des articles 122 et 123 de la loi du 13 juin 2005; enfin, ils sont tenus d'assurer une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données par une autorité habilitée à ce faire, cette traçabilité étant effectuée à l'aide d'un journal, que l'IBPT et la Commission pour la protection de la vie privée peuvent consulter ou dont ils peuvent exiger une copie en tout ou en partie[37].

3.4.2. Des éléments qui précèdent, il ressort que le texte en projet met en place un système extrêmement précis et complet de nature à assurer en droit, et en fait, la pleine intégrité et la confidentialité des données ainsi que leur destruction irrémédiable au terme de leur durée de conservation, système se caractérisant "par un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles"[38].

Toutefois, afin de répondre pleinement aux exigences qui résultent à ce titre de l'arrêt de la Cour de Justice, le texte en projet gagnerait à être revu sur quelques aspects.

3.4.2.1. Il résulte de l'article 126/1, § 1er, alinéa 4, en projet, que le Roi est habilité par arrêté délibéré en Conseil des ministres, à dispenser certaines catégories d'opérateurs et fournisseurs des exigences imposées aux membres de la Cellule de coordination, relatives à l'avis de sécurité et à l'absence de refus du ministre de la Justice, telles qu'elles sont prévues par l'alinéa 3 du même paragraphe, ou de fixer des conditions moins strictes pour ces catégories.

Le commentaire de l'article expose à ce sujet que

"Il est toutefois nécessaire de prendre en compte le fait que, en fonction de l'évolution des acteurs, le projet de loi peut s'appliquer à des fournisseurs ou opérateurs de petite taille pour lesquels certaines de ces vérifications deviennent

[37] Article 126, § 4, en projet.
[38] C.J.U.E., n° C-293/12, arrêt Digital Rights Ireland Ltd, pt 67.

worden. Het wetsontwerp voorziet dus in de mogelijkheid om bepaalde categorieën van operatoren of aanbieders vrij te stellen van deze verplichtingen of voorwaarden."

Bovendien bepaalt artikel 126/1, § 3, tweede lid, dat de Koning bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, mag bepalen bij welke categorieën van aanbieders of operatoren de aangestelde voor de bescherming van de persoonsgegevens wel lid mag zijn van de Coördinatiecel.[39]

In de bespreking van het artikel wordt daaromtrent het volgende gezegd:

"Er moet echter rekening worden gehouden met het feit dat afhankelijk van de evolutie van de actoren, het wetsontwerp van toepassing kan zijn op kleine aanbieders of operatoren, voor wie deze incompatibiliteit, die inhoudt dat twee verschillende personen moeten worden aangewezen voor de Coördinatiecel en voor de functie van aangestelde voor de bescherming van de gegevens, disproportioneel wordt. Het wetsontwerp voorziet dus in de mogelijkheid om een uitzondering te maken voor sommige categorieën van operatoren of aanbieders."

Hoewel het doel dat door de steller van het voorontwerp wordt nagestreefd, namelijk dat geen onevenredige of onmogelijk na te komen verplichtingen worden opgelegd aan operatoren en aanbieders die over weinig personeel beschikken, als legitiem kan worden beschouwd, mag de ingevoerde regeling er niet toe leiden dat de personen op wie de bewaarde gegevens betrekking hebben, verstoken blijven van een aantal waarborgen die het voorontwerp aan hen biedt op het stuk van de bescherming van een fundamenteel recht, het recht op eerbieding van het privéleven, louter en alleen omdat de operator of de aanbieder die die gegevens bewaart, "klein" is.

Het ontwerp moet aldus worden herzien dat iedereen vergelijkbare waarborgen krijgt ongeacht de grootte van de betrokken operatoren of aanbieders, bijvoorbeeld onder meer via de mogelijkheid die het ontwerp reeds aan de operatoren biedt om een gemeenschappelijke Coördinatiecel op te richten.

Het staat hoe dan ook aan de wetgever om te bepalen met welke criteria de Koning rekening moet houden om uitvoering te geven aan de hem verleende machtiging.

3.4.2.2. Het ontworpen artikel 126, § 4, 6°, bepaalt dat de gegevens na afloop van de bewaringstermijn van elke drager moeten worden verwijderd.

3.4.2.2.1. Die verwijdering vindt evenwel plaats "onverminderd de artikelen 122 en 123".

[39] Op het eerste gezicht lijken die machtigingen herhaald te worden in artikel 126/1, § 4, 1° en 4°. Wat betreft de bedoeling van de steller van het voorontwerp en de problemen die ontstaan door de cumulatie of de dubbele vermelding van al deze machtigingen die aan de Koning worden verleend, wordt verwezen naar de bijzondere opmerkingen die hierna worden gemaakt met betrekking tot artikel 5 van het voorontwerp.

disproportionnées. Le projet de loi prévoit donc la possibilité d'exonérer certaines catégories d'opérateurs ou de fournisseurs de ces obligations ou conditions".

Par ailleurs, l'article 126/1, § 3, alinéa 2, permet au Roi, par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée, de déterminer des catégories de fournisseurs ou d'opérateurs pour lesquels le préposé à la protection des données à caractère personnel peut être membre de la Cellule de coordination[39].

Le commentaire de l'article mentionne à ce propos que

"Il est toutefois nécessaire de prendre en compte le fait que, en fonction de l'évolution des acteurs, le projet de loi peut s'appliquer à des fournisseurs ou opérateurs de petite taille pour lesquels cette incompatibilité, qui implique de désigner deux personnes différentes pour la Cellule de coordination et pour la fonction de préposé à la protection des données, devient disproportionnée. Le projet de loi prévoit donc la possibilité de créer une exception pour certaines catégories d'opérateurs ou de fournisseurs".

Si l'on peut considérer comme légitime le but poursuivi par l'auteur de l'avant-projet, à savoir ne pas imposer d'obligations disproportionnées ou irréalisables aux opérateurs et fournisseurs disposant de peu de personnel, le système mis en place ne peut aboutir au fait de priver les personnes auxquelles les données conservées, sont relatives de certaines garanties que l'avant-projet leur donne en termes de protection d'un droit fondamental, celui du respect de la vie privée, pour la seule raison que l'opérateur ou le fournisseur qui conserve ces données serait "de petite taille".

Le texte en projet sera revu de manière à prévoir des garanties équivalentes pour tous, quelle que soit la taille des opérateurs ou fournisseurs concernés et ce notamment par le biais, par exemple, de la possibilité déjà offerte par le texte en projet aux opérateurs de constituer une Cellule de coordination commune.

En tout état de cause, c'est au législateur qu'il appartient de fixer les critères à prendre en considération par le Roi pour mettre en œuvre son habilitation.

3.4.2.2. La destruction des données au terme du délai de conservation est imposée par l'article 126, § 4, 6°, en projet.

3.4.2.2.1. Toutefois, cette destruction s'effectue "sans préjudice des articles 122 et 123".

[39] À la première lecture, ces habilitations semblent être rappelées par l'article 126/1, § 4, 1° et 4°. Sur l'intention de l'auteur de l'avant-projet et les difficultés soulevées par le cumul ou la conjonction de l'ensemble de ces habilitations données au Roi, il est renvoyé aux observations particulières faites ci-après sous l'article 5 de l'avant-projet.

In de bespreking van het artikel wordt daaromtrent het volgende uiteengezet: “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.”

De vraag rijst of het niet beter zou zijn te bepalen dat de gegevens die krachtens het ontworpen artikel 126 bewaard worden, bewaard moeten worden in een databank die enkel bedoeld is voor die gegevens om het gevaar dat de desbetreffende gegevens niet verwijderd worden zoveel mogelijk in te perken.

3.4.2.2.2. De ontworpen bepalingen zouden beter tegemoetkomen aan de vereisten inzake de onherroepelijke vernietiging van de gegevens indien een overheidsinstantie, zoals het BIPT, specifiek belast zou worden met de controle op de daadwerkelijke en onherroepelijke vernietiging van de gegevens.

Weliswaar is het BIPT krachtens artikel 14, § 1, 3°, van de wet van 17 januari 2003 “met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector” in het algemeen belast met het toezicht op de naleving van de wet van 13 juni 2005 in haar geheel en kan de Koning aan de statutaire personeelsleden van het Instituut de hoedanigheid verlenen van officier van gerechtelijke politie, die overeenkomstig de artikelen 24 en 25 van dezelfde wet van 17 januari 2003 over heel wat bevoegdheden beschikt. Bovendien verleent het ontworpen artikel 126, § 2, eerste lid, 3° aan elke officier van gerechtelijke politie van het BIPT toegang tot de desbetreffende gegevens met het oog op het opsporen, het onderzoek en de vervolging van onder meer inbreuken op het ontworpen artikel 126.

De afdeling Wetgeving wijst er evenwel op dat bijvoorbeeld in geen enkele strafbaarstelling is voorzien met betrekking tot het niet vernietigen van gegevens na het verstrijken van de bewaartermijn. Zo ook verplicht geen enkele bepaling het BIPT om op dat vlak regelmatig specifieke controles uit te voeren. Zulke bepalingen zouden evenwel een grotere garantie bieden dat de gegevens daadwerkelijk vernietigd worden.

3.4.2.2.3. De ontworpen tekst dient in het licht van deze opmerkingen te worden herzien.

3.5. Het feit dat het ontwerp de verplichting wordt opgelegd, om de desbetreffende gegevens op het grondgebied van de Unie te bewaren.

Luidens het ontworpen artikel 126, § 4, 4°, moeten de betrokken aanbieders en operatoren “de gegevens op het grondgebied van de Europese Unie (...) bewaren”.

Le commentaire de l’article expose, à ce propos, qu’“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 être conservée sur base des articles 122 et 123 de la loi”.

Afin de limiter de manière maximale les risques de non-destruction des données concernées, la question se pose de savoir s’il ne serait pas adéquat de prévoir que les données conservées en vertu de l’article 126 en projet doivent l’être dans une base de données exclusivement consacrées à ces données.

3.4.2.2.2. Le dispositif en projet répondrait mieux aux exigences relatives à la destruction irrémédiable des données si une autorité, telle l’IBPT, était spécifiquement chargée de contrôler la destruction effective et irrémédiable des données.

Certes, l’IBPT est, de manière générale, chargé du contrôle du respect de l’ensemble de la loi du 13 juin 2005 en vertu de l’article 14, § 1er, 3°, de la loi du 17 janvier 2003 “relative au statut du régulateur des secteurs des postes et des télécommunications belges” et le Roi peut conférer aux membres statutaires du personnel de l’Institut, la qualité d’officier de police judiciaire disposant de nombreux pouvoirs, conformément aux articles 24 et 25 de la même loi du 17 janvier 2003. Par ailleurs, l’article 126, § 2, alinéa 1er, 3°, en projet permet à tout officier de police judiciaire de l’IBPT d’accéder aux données concernées en vue de la recherche, de l’instruction et de la poursuite d’infractions notamment à l’article 126 en projet.

Toutefois, la section de législation relève, à titre d’exemples, qu’il n’est prévu aucune incrimination pénale en matière de non-destruction des données au terme de leur délai de conservation. De même, aucune disposition n’impose à l’IBPT d’effectuer des contrôles réguliers et spécifiques en la matière. Or, de telles dispositions permettraient sans doute de mieux garantir l’effectivité de la destruction des données.

3.4.2.2.3. Le dispositif en projet sera réexaminé à la lumière de ces observations.

3.5. Quant au fait que le texte en projet impose la conservation des données en cause sur le territoire de l’Union

L’article 126, § 4, 4°, en projet prévoit que les fournisseurs et les opérateurs concernés “conservent les données sur le territoire de l’Union européenne”.

BIJZONDERE OPMERKINGEN

INDIENINGSBESLUIT

Het indieningsbesluit dient te worden gesteld als volgt:

“FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

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

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Digitale Agenda, Telecommunicatie en Post, de minister van Justitie en de minister van Defensie zijn ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen:”.[40]

DISPOSITIEF

Artikel 4

1. Artikel 4 van het voorontwerp strekt ertoe artikel 126 van de wet van 13 juni 2005 te vervangen.

Naast de bovenstaande algemene opmerkingen, behoren bij die bepaling de volgende opmerkingen te worden gemaakt.

1.1. Het ontworpen artikel 126, § 2, eerste lid, bepaalt dat de operatoren en aanbieders de gegevens mededelen op “eenvoudig verzoek” van de overheden die toegang kunnen krijgen tot die gegevens om de redenen die in die bepaling worden opgesomd en binnen de termijn die hun daartoe eventueel is toegemeten.

In de bespreking van het artikel staat in dat verband het volgende: “Dit betekent geenszins dat de voorwaarden die opgenomen zijn in bijvoorbeeld de artikelen 46*bis* en 88*bis* 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”.

1.2. Wat anderzijds de aanvragen betreft die krachtens het ontworpen artikel 126, § 2, eerste lid, 4°, door de hulpdiensten worden gedaan, wordt de betrokken aanbieder of operator verplicht “een voorafgaande controle […] van de identiteit van de hulpdiensten” uit te voeren. In de bespreking van het artikel wordt daarvoor de volgende uitleg gegeven:

[40] *Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbeveling 226 en 227, formule F 5.

OBSERVATIONS PARTICULIÈRES

ARRÊTÉ DE PRÉSENTATION

L’arrêté de présentation sera rédigé comme suit:

“PHILIPPE, Roi des Belges,

À tous, présents et à venir, Salut.

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, le ministre de la Justice et le ministre de la Défense sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:”[40].

DISPOSITIF

Article 4

1. L’article 4 de l’avant-projet entend remplacer l’article 126 de la loi du 13 juin 2005.

Outre les observations générales ci-avant, cette disposition appelle les observations suivantes.

1.1. L’article 126, § 2, alinéa 1er, en projet prévoit que les opérateurs et fournisseurs communiquent les données sur “simple demande” des autorités habilitées à avoir accès à ces données pour les finalités y énumérées et dans le délai qui leur est éventuellement imparti pour ce faire.

Le commentaire de l’article mentionne à ce propos que “cela ne signifie nullement que les conditions prévues par exemple par les articles 46*bis* et 88*bis* 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”.

1.2. Par ailleurs, s’agissant des demandes adressées par les services d’urgence en vertu de l’article 126, § 2, alinéa 1er, 4°, en projet, il est imposé au fournisseur ou à l’opérateur concerné d’“effectue[r] une vérification préalable de l’identité des services d’urgence”. Le commentaire de l’article s’en explique comme suit:

[40] *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet “Technique législative”, recommandations nos 226 et 227, formule F 5.

"Deze paragraaf verplicht de operator of aanbieder [...] 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. Het spreekt voor zich dat de hulpdiensten die ter plaatse hulp bieden en de operatoren samen veiligheidsmechanismen moeten overeenkomen, waarbij elke partij haar verantwoordelijkheid neemt om een misbruik van identiteit te voorkomen".

Hoewel bij de ontworpen regeling geen enkele vergelijkbare verplichting wordt opgelegd in het geval van een aanvraag komende van de Cel Vermiste Personen van de federale politie, wordt in de bespreking van het artikel daarover niettemin het volgende gezegd:

"Net zoals het geval is voor de samenwerking met de hulpdiensten die ter plaatse hulp bieden, komen de operatoren en de Cel vermiste personen van de federale politie modaliteiten of praktische procedures overeen teneinde te garanderen dat de operatoren effectief in contact staan met de bevoegde officier van de gerechtelijke politie."

2. Gelet op de bewoordingen waarin de bepaling is gesteld, en gelet op de bovenstaande uitleg gegeven in de bespreking van het artikel, geeft de voorliggende bepaling aanleiding tot de volgende opmerkingen.

Ingeval een aanvraag steunt op een handeling van een gerechtelijke overheid of van de inlichtingendiensten, moet die handeling, per definitie, en krachtens de ontworpen tekst,[41] al beantwoorden aan de voorwaarden die, naargelang het geval, worden opgesomd in de artikelen 46*bis* of 88*bis* van het Wetboek van Strafvordering of in de relevante bepalingen van de wet van 30 november 1998.

In de andere gevallen wordt bij de ontworpen tekst geen enkele formele voorwaarde gesteld, en in de bespreking van de artikelen wordt, overigens alleen voor bepaalde gevallen,[42] gezegd dat enerzijds de aanbieders en de operatoren, en anderzijds de overheden die toegang vragen tot de gegevens, de modaliteiten en praktische procedures moeten uitwerken om zich ervan te vergewissen dat de aanvraag wel degelijk uitgaat van een gemachtigde overheid.

De beoordeling van een kwestie die dermate belangrijk is bij het voorkomen van onregelmatige en onrechtmatige aanvragen en die als doel heeft te vermijden dat een niet gemachtigd persoon toegang zou kunnen hebben tot de bewaarde gegevens, mag niet worden overgelaten aan de betrokkenen. Bovendien kan ook niet zonder meer worden bepaald dat de aanbieder of de operator, die beide helemaal

"[...] 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. Il va de soi que les services d'urgence offrant de l'aide sur place et les opérateurs doivent convenir ensemble de ces mécanismes de sécurité, chaque partie devant prendre ses responsabilités pour éviter une usurpation d'identité".

Alors qu'aucune obligation similaire n'est imposée par le dispositif en projet en cas de demande émanant de la cellule de disparition de la police fédérale, le commentaire de l'article ajoute néanmoins à ce propos:

"Tout comme pour la collaboration avec les services d'urgence offrant de l'aide sur place, les opérateurs et la cellule de disparition de la police fédérale conviendront de modalités ou de procédures pratiques pour garantir que les opérateurs sont bien en contact avec l'officier compétent de la police judiciaire".

2. Compte tenu des termes dans lesquelles elle est rédigée, et des explications ainsi données dans le commentaire de l'article, la disposition à l'examen appelle les observations suivantes.

Dans le cas où la demande trouve son fondement dans un acte d'une autorité judiciaire ou des services de renseignement, cet acte doit déjà, par définition, et en vertu du texte en projet[41], répondre aux conditions prévues selon le cas, aux articles 46*bis* ou 88*bis* du Code d'instruction criminelle, ou aux dispositions pertinentes de la loi du 30 novembre 1998.

Dans les autres cas, le texte en projet n'impose aucune exigence formelle, et le commentaire des articles expose, au surplus pour certaines hypothèses seulement[42], que les opérateurs et les fournisseurs d'une part, et les autorités qui demandent l'accès aux données, d'autre part, devront trouver les modalités et procédures pratiques permettant de s'assurer que la demande émane bien d'une autorité habilitée.

Une question aussi fondamentale dans la prévention des demandes irrégulières ou abusives, qui a pour objet d'éviter qu'une personne non habilitée puisse avoir accès aux données conservées, ne peut être laissée à l'appréciation des intervenants. Par ailleurs, il ne peut être prévu, sans autre précision, et alors que ceux-ci ne disposent pas de et ne peuvent se voir attribuer aucun pouvoir de police, que le

41 Zie de woorden "en volgens de voorwaarden bepaald in die artikelen", die worden gebruikt in het ontworpen artikel 126, § 2, eerste lid, 1° en 2°.

42 In de ontworpen tekst wordt niets gezegd in verband met de aanvragen uitgaande van de Ombudsdienst voor telecommunicatie, en dat terwijl de aanvraag van die dienst volgt op een klacht van "elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een [ ] netwerk of dienst" en, bijgevolg, op een verzoek van een privépersoon en niet van een overheid.

41 Voir les mots "et dans les conditions fixées par ces articles", employés dans l'article 126, § 2, alinéa 1er, 1° et 2°, en projet.

42 Le texte en projet est muet en ce qui concerne les demandes d'accès émanant du Service de médiation pour les télécommunications et ce, alors que la demande de ce Service fait suite à une plainte de "toute personne se prétendant victime d'une utilisation malveillante d'un réseau et d'un service", et , par conséquent, à la demande d'un particulier et non d'une autorité.

geen politiebevoegdheid hebben en die ook niet kunnen krijgen, "een voorafgaande controle […] van de identiteit van de hulpdiensten" uitvoeren, zoals in de ontworpen tekst staat.

De ontworpen tekst dient dan ook zodanig te worden aangevuld dat daarbij, tenminste voor de gevallen waar die garantie niet reeds voortvloeit uit andere wetsbepalingen, de Koning uitdrukkelijk wordt gemachtigd de inhoud en de vorm van de aanvraag vast te leggen, zodat de operatoren en de aanbieders op basis van die aanvraag er zeker van mogen zijn dat ze wel degelijk uitgaat van een overheid of een persoon die gemachtigd is om toegang tot de gegevens te vragen voor de doeleinden waarvoor en onder de voorwaarden waaronder het ontworpen artikel 126 die toegang toestaat.

Bijgevolg dient de laatste zin van het ontworpen artikel 126, § 2, eerste lid, 4°, te worden weggelaten en dient de bespreking van het artikel te worden herzien. De machtiging die bij het ontworpen artikel 126/1, § 4, 6°,[43] aan de Koning wordt verleend, dient eveneens te worden herzien en dient te worden aangevuld in het licht van deze opmerkingen.

Artikel 5

Los van de bovenstaande algemene opmerkingen en onder voorbehoud daarvan, behoren bij de voorliggende bepaling de volgende opmerkingen te worden gemaakt.

1. Zoals hierboven vermeld, bepaalt het ontworpen artikel 126/1, § 1, vierde lid, dat

"de Koning (…), bij een in Ministerraad overlegd besluit, [kan] beslissen dat bepaalde categorieën van operatoren of aanbieders niet onderworpen zijn aan de voorwaarden die worden beoogd in het derde lid[44] of (…) voor deze categorieën minder strikte voorwaarden [kan] vastleggen".

Het ontworpen artikel 126/1, § 3, tweede lid, dat betrekking heeft op de "aangestelde voor de bescherming van de persoonsgegevens" bepaalt zijnerzijds:

"Deze aangestelde mag geen deel uitmaken van de Coördinatiecel. De Koning mag evenwel, bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de categorieën bepalen van aanbieders of operatoren waarvoor deze onverenigbaarheid niet van toepassing is".

De bepalingen onder 1° en 4° van het ontworpen artikel 126/1, § 4, luiden dan weer als volgt:

fournisseur ou l'opérateur effectue une "vérification préalable de l'identité des services d'urgence", comme le texte en projet le mentionne.

Dès lors, le texte en projet sera complété de sorte qu'en tout cas pour les hypothèses où cette garantie ne résulte pas déjà d'autres dispositions législatives, il habilite expressément le Roi à définir le contenu et la forme de la demande, de manière que, sur la base de celle-ci, les opérateurs et les fournisseurs puissent être assurés que celle-ci émane bien d'une autorité ou d'une personne habilitée à demander l'accès aux données, aux fins pour lesquelles et dans les conditions auxquelles l'article 126 en projet autorise cet accès.

En conséquence, à l'article 126, § 2, alinéa 1er, 4°, en projet, la dernière phrase sera omise, et le commentaire de l'article sera revu. De même, l'habilitation conférée au Roi par l'article 126/1, § 4, 6°[43], en projet, sera utilement revue et complétée à la lumière de ces observations.

Article 5

Outre les observations générales ci-avant et sous réserve de celles-ci, la disposition à l'examen appelle les observations suivantes.

1. Comme mentionné ci-avant, l'article 126/1, § 1er, alinéa 4, en projet, prévoit que

"Le Roi peut, par arrêté délibéré en Conseil des ministres, décider que certaines catégories d'opérateurs ou fournisseurs ne sont pas soumises aux conditions visées au troisième alinéa[44] ou fixer pour ces catégories des conditions moins strictes".

L'article 126/1, § 3, alinéa 2, en projet, qui a trait au "préposé à la protection des données à caractère personnel" prévoit quant à lui, que

"Ce préposé ne peut pas faire partie de la Cellule de coordination. Le Roi peut toutefois, par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée, déterminer les catégories de fournisseurs ou d'opérateurs pour lesquels cette incompatibilité n'est pas applicable".

Pour sa part, l'article 126/1, § 4, en projet, prévoit, en ses 1° et 4°, que

[43] Die bepaling machtigt de Koning tot het vaststellen van "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".

[44] Namelijk de verplichting dat de leden van de Coördinatiecel over een niet-achterhaald positief veiligheidsadvies beschikken en niet geweigerd zijn door de minister van Justitie.

[43] Par cette disposition le Roi est habilité à déterminer "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".

[44] À savoir l'obligation, pour les membres de la Cellule de coordination, de disposer d'un avis de sécurité positif non périmé et de ne pas avoir fait l'objet d'un refus du ministre de la Justice.

"§ 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:

1° de categorieën van operatoren en de categorieën van aanbieders bedoeld in artikel 126, § 1, eerste lid, die zijn vrijgesteld van bepaalde eisen vastgelegd in paragraaf 1;

(...)

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;".

Die bepalingen zijn problematisch om de volgende redenen:

Als de machtigingen die zijn opgenomen in paragraaf 4, 1° en 4°, enkel tot doel hebben de machtigingen in herinnering te brengen die respectievelijk verleend worden in paragraaf 1, vierde lid, en paragraaf 3, tweede lid,

1° zijn ze enerzijds een herhaling ervan en bijgevolg overbodig;

2° verschillen ze anderzijds hoe dan ook van de machtigingen die ze in herinnering zouden moeten brengen;

— wordt in paragraaf 4, naast het overleg in de Ministerraad voorgeschreven in paragraaf 1, vierde lid, het advies vereist van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het BIPT;

— is paragraaf 4, 1° gesteld in vage bewoordingen in zoverre hij de Koning de mogelijkheid biedt de categorieën van aanbieders en operatoren te bepalen die zijn vrijgesteld van "bepaalde eisen vastgelegd in paragraaf 1", terwijl paragraaf 1, vierde lid, nauwkeuriger is geformuleerd, aangezien daarbij aan de Koning de mogelijkheid wordt geboden de categorieën te bepalen die "niet onderworpen zijn aan de voorwaarden die worden beoogd in het derde lid" of "voor deze categorieën minder strikte voorwaarden" vast te leggen;

— wordt in paragraaf 4, 4° de Koning gemachtigd categorieën te bepalen van aanbieders en operatoren "die zijn vrijgesteld van de naleving van een deel of van het geheel van paragraaf 3", terwijl de eventuele vrijstelling zoals bedoeld in paragraaf 3, tweede lid, enkel betrekking heeft op het vereiste dat de aangestelde voor de bescherming van persoonsgegevens geen lid mag zijn van de Coördinatiecel.

Als de machtigingen vervat in paragraaf 4, 1° en 4°, tot doel hebben aan de Koning de bevoegdheid te verlenen om te

"§ 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° les catégories d'opérateurs et les catégories de fournisseurs visés à l'article 126, § 1er, alinéa, 1er, qui sont dispensés de certaines exigences fixées au paragraphe 1er;

[...]

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;".

Ces dispositions posent des difficultés pour les motifs suivants:

Si les habilitations qui figurent au paragraphe 4, 1° et 4°, ont pour seul objet de rappeler celles qui figurent respectivement, au paragraphe 1er, alinéa 4, et paragraphe 3, alinéa 2, alors:

1° d'une part, elles font double emploi avec celles-ci et sont inutiles;

2° d'autre part et en tout état de cause, elles diffèrent des habilitations qu'elles sont censées rappeler; ainsi:

— le paragraphe 4, exige, outre la délibération en Conseil des ministres requise par le paragraphe 1er, alinéa 4, l'avis de la Commission pour la protection de la vie privée et celui de l'IBPT;

— le paragraphe 4, 1°, est rédigé en des termes vagues en ce qu'il permet au Roi de déterminer les catégories d'opérateurs et de fournisseurs qui sont dispensées "de certaines exigences fixées au paragraphe 1er", alors que le paragraphe 1er, alinéa 4, permet au Roi, de manière plus précise, de déterminer les catégories qui "ne sont pas soumises aux conditions visées au troisième alinéa ou fixer pour ces catégories des conditions moins strictes";

— le paragraphe 4, 4°, habilite le Roi à déterminer les catégories d'intervenants "qui sont dispensés du respect du paragraphe 3, en tout ou en partie", tandis que la dispense éventuelle prévue au paragraphe 3, alinéa 2, porte uniquement sur l'obligation pour le préposé à la protection de données à caractère personnel de ne pas être membre de la Cellule de coordination.

Si les habilitations qui figurent au paragraphe 4, 1° et 4°, ont pour objet de conférer au Roi le pouvoir de prévoir

voorzien in andere vrijstellingen en afwijkingen dan die waarin respectievelijk al in paragraaf 1, vierde lid, en paragraaf 3, tweede lid is voorzien[45], moet worden vastgesteld dat wat die machtigingen betreft, niet wordt gepreciseerd wie wordt vrijgesteld en waarvan juist vrijstelling wordt verleend.

Wat ook de bedoeling is van de steller van het voorontwerp, hij dient de aldus gesignaleerde dubbelzinnigheden of contradicties weg te werken zodanig dat, onder voorbehoud van de bovenstaande algemene opmerkingen, het voorwerp van die machtigingen welomlijnd en duidelijk is, waarbij hij overlapping tussen de verschillende machtigingen die hij wenst te verlenen moet vermijden. Zoals overigens reeds is opgemerkt, moet de wetgever de criteria bepalen die de Koning moet hanteren wanneer hij zijn machtiging ten uitvoer legt, alsook het precieze voorwerp ervan, teneinde te waarborgen dat het gelijkheidsbeginsel en het recht op de eerbiediging van de persoonlijke levenssfeer van de personen van wie de gegevens worden bewaard, in acht worden genomen.

De voorliggende bepaling moet dienovereenkomstig worden herzien.

2. In het ontworpen artikel 126/1, § 3, vijfde lid, dient te worden verduidelijkt wat moet worden verstaan onder het begrip “management”.

Artikel 8

1. De vraag rijst wat de exacte strekking is van de beperking zoals bedoeld in het ontworpen artikel 46*bis*, § 1, vierde lid, van het Wetboek van Strafvordering: kan de procureur des Konings toegang krijgen tot de bewaarde gegevens voor een beperkte periode van zes maanden voorafgaand aan zijn beslissing voor alle strafbare feiten behalve die welke een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben, voor welke strafbare feiten de termijn wordt uitgebreid tot twaalf maanden,[46] of moet die bepaling – en zulks is waarschijnlijker – gelet op het ontworpen artikel 88*bis*, § 1, eerste lid, van het Wetboek van Strafvordering, zo worden begrepen dat aan de procureur enkel toegang wordt verleend tot die gegevens in het kader van strafbare feiten die een correctionele hoofdgevangenisstraf tot gevolg kunnen hebben, met dien verstande dat wanneer de correctionele hoofdgevangenisstraf één jaar of meer bedraagt, de termijn wordt uitgebreid tot twaalf maanden?

De voorliggende bepaling dient aldus te worden herzien dat elke dubbelzinnigheid dienaangaande wordt weggewerkt.

2. De afdeling Wetgeving vraagt zich voorts ook af waarom

[45] Dat geval is geenszins uit te sluiten aangezien in de bespreking van het artikel het volgende wordt vermeld: “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.”

[46] Aangezien de bewaringstermijn precies twaalf maanden is.

d’autres dispenses ou dérogations que celles déjà prévues[45], respectivement, au paragraphe 1er, alinéa 4, et paragraphe 3, alinéa 2, alors il faut constater que ces habilitations ne précisent pas quels seront l’objet et les destinataires des dispenses considérées.

Quelle que soit l’intention de l’auteur de l’avant-projet, il lui appartient de lever les ambiguïtés ou contradictions ainsi relevées, de sorte que, sous réserve des observations générales ci-avant, ces habilitations portent sur des objets précis et clairement identifiables, en évitant tout double emploi entre les différentes habilitations envisagées. Par ailleurs, comme déjà observé, il appartient au législateur de déterminer les critères à mettre en œuvre par le Roi lorsqu’il fait usage de son habilitation, ainsi que les objets précis sur lesquelles elle porte, de manière à garantir le respect du principe d’égalité et du droit au respect de la vie privée des personnes dont les données sont conservées.

La disposition à l’examen sera revue en conséquence.

2. À l’article 126/1, § 3, alinéa 5, en projet, il convient de mieux préciser ce que l’on entend par “management”.

Article 8

1. La question se pose de savoir quelle est la portée exacte de la limitation de six mois prévue par l’article 46*bis*, § 1er, alinéa 4, en projet, du Code d’instruction criminelle: le procureur du Roi est-il habilité à accéder aux données conservées pendant un délai restreint de six mois avant sa décision pour toutes les infractions sauf celles qui peuvent donner lieu à une peine d’emprisonnement correctionnel principal d’un an ou une peine plus lourde, infractions pour lesquelles le délai est étendu à douze mois[46], ou bien, plus probablement, compte tenu de l’article 88*bis*, § 1er, alinéa 1er, en projet, du Code d’instruction criminelle, faut-il comprendre cette disposition comme lui permettant l’accès à ces données uniquement dans le cadre d’infractions pouvant donner à lieu une peine d’emprisonnement correctionnel principal, étant entendu que lorsque la peine d’emprisonnement correctionnel principal atteint ou dépasse un an, le délai est étendu à douze mois?

La disposition à l’examen sera revue de manière à lever toute ambiguïté à ce propos.

2. Par ailleurs, la section de législation s’interroge sur les

[45] Cette hypothèse n’est nullement à écarter puisque le commentaire de l’article mentionne “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”.

[46] Dès lors que le délai de conservation est précisément de douze mois.

in de ontworpen tekst niet hetzelfde onderscheid wordt gemaakt als dat waarin is voorzien in het ontworpen artikel 88*bis*, § 2, van hetzelfde wetboek, waaruit volgt dat de toegang beperkt is tot 12 of 9 maanden naargelang de situatie een strafbaar feit betreft "bedoeld in Titel I*ter* van Boek II van het Strafwetboek", dan wel een ander strafbaar feit zoals bedoeld in artikel 90*ter*, § 2 tot § 4 van hetzelfde wetboek, een strafbaar feit dat begaan is in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een correctionele hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben.

Volgens de uitleg die de gemachtigde van de minister heeft gegeven, zouden die verschillen tussen de twee ontworpen bepalingen voornamelijk te wijten zijn aan het feit dat bij artikel 46*bis*, § 1, van het Wetboek van Strafvordering de procureur des Konings enkel toegang krijgt tot de gegevens voor de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst voor elektronische communicatie of van het gebruikte middel voor elektronische communicatie en voor de identificatie van de diensten voor elektronische communicatie waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden, terwijl bij artikel 88*bis* van hetzelfde wetboek de onderzoeksrechter toegang krijgt tot ruimere en volledigere gegevens, aangezien de onderzoeksrechter de oproepgegevens kan laten opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan, alsook de oorsprong of de bestemming van telecommunicatie kan laten lokaliseren.[47]

Hoewel inderdaad aanvaard kan worden dat de beperking van de toegang in de tijd zoals bepaald in het ontworpen artikel 88*bis*, § 2, en die waarin is voorzien in het ontworpen artikel 46*bis*, § 1, vierde lid, verschillen gelet op de inhoud zelf van de betrokken gegevens, moet wat betreft het verschil in behandeling niettemin met nog twee andere zaken rekening worden gehouden: vooreerst betreft artikel 46*bis* de toegang van het openbaar ministerie tot de gegevens, terwijl artikel 88*bis* de toegang van de onderzoeksrechter tot de gegevens betreft;[48] vervolgens volgt uit het ontworpen artikel 126, § 3, dat de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen "gedurende twaalf maanden [worden] bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst", met als gevolg dat als de toegang van de procureur des Konings tot de gegevens niet door de ontworpen tekst in de tijd wordt beperkt, die toegang *de facto* uitgebreid zou kunnen worden tot een periode van meer dan twaalf maanden, aangezien de gegevens worden bewaard voor een termijn waarvan het verstrijken pas ingaat vanaf het ogenblik dat communicatie niet mogelijk is via de gebruikte dienst.

In de memorie van toelichting moet derhalve specifieker worden uitgelegd waarom twee gevallen van beperking van

47 De procureur des Konings kan dergelijke maatregelen alleen bevelen in spoedeisende gevallen en enkel voor bepaalde strafbare feiten, en die maatregel moet binnen vierentwintig uur worden bekrachtigd door een onderzoeksrechter (artikel 88*bis* van het Wetboek van Strafvordering).

48 Wat overigens verklaart waarom de gegevens waartoe de betrokken overheid toegang heeft, verschillen van de ene bepaling tot de andere.

motifs pour lesquels le texte en projet n'opère pas également la distinction prévue par l'article 88*bis*, § 2, en projet, du même code, dont il résulte des accès limités à 12 ou 9 mois, selon que la situation concerne une infraction "visée au Titre I*ter* du Livre II du Code pénal" ou bien que l'on se trouve dans une situation d'infraction autre visée à l'article 90*ter*, § § 2 à 4 du même code, ou qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou qui est de nature à entraîner une peine d'emprisonnement correctionnel principal de cinq ans ou une peine plus lourde.

Selon les explications communiquées par le délégué du ministre, ces différences entre les deux dispositions en projet seraient dues essentiellement au fait que l'article 46*bis*, § 1er, du Code d'instruction criminelle permet au procureur du Roi d'avoir accès uniquement aux données d'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communications électroniques utilisé, et d'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, tandis que l'article 88*bis* du même code permet au juge d'instruction d'avoir accès à des données plus larges et complètes puisque le juge d'instruction peut ordonner le repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, ainsi que la localisation de l'origine ou de la destination de télécommunications[47].

Si l'on peut effectivement admettre que les limitations de l'accès dans le temps prévues à l'article 88*bis*, § 2, en projet et celles prévues à l'article 46*bis*, § 1er, alinéa 4, en projet, diffèrent, compte tenu de l'objet même des données concernées, la différence de traitement opérée doit néanmoins tenir compte de deux éléments supplémentaires: tout d'abord, l'article 46*bis* concerne l'accès aux données par le ministère public, tandis que l'article 88*bis* concerne l'accès aux données par le juge d'instruction[48]; ensuite, il résulte de l'article 126, § 3, en projet, que les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication 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", avec pour conséquence que si l'accès du procureur du Roi aux données n'est pas limité dans le temps par le texte en projet, il pourrait s'en trouver *de facto* étendu à une période supérieure à douze mois, les données étant conservées dans un délai dont l'expiration ne prend cours qu'à dater du moment où une communication n'est pas possible à l'aide du service utilisé.

L'exposé des motifs doit dès lors mieux faire apparaître les justifications du fait que deux hypothèses de limitation d'accès

47 Le procureur du Roi ne peut ordonner des mesures similaires qu'en cas d'urgence et pour certaines infractions seulement, et cette mesure doit être confirmée dans les vingt-quatre heures par un juge d'instruction (article 88*bis* du Code d'instruction criminelle).

48 Ce qui justifie d'ailleurs que les données auxquelles l'autorité concernée a accès diffèrent d'une disposition à l'autre.

de toegang in de tijd waarin wordt voorzien in het ontworpen artikel 88*bis*, § 2, niet zijn opgenomen in het ontworpen artikel 46*bis*, § 1, vierde lid.

Artikel 9

1. Al worden, zoals de gemachtigde van de minister heeft aangegeven, wat betreft de opsomming van de betreffende strafbare feiten, in het ontworpen artikel 88*bis*, § 2, tweede streepje, bestaande bepalingen overgenomen,[49] lijkt het toch beter, teneinde de bedoeling van de steller van het voorontwerp getrouwer weer te geven, dat artikel 88*bis*, § 2, tweede streepje, gesteld wordt als volgt:

"– Voor andere strafbare feiten bedoeld in artikel 90*ter*, § § 2 tot 4, of strafbare feiten die niet opgenomen zijn in die bepaling en gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of strafbare feiten die een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben (voorts zoals in het voorontwerp);".

2. Bij artikel 9 van het voorontwerp wordt een nieuwe paragraaf 3 ingevoegd in artikel 88*bis* van het Wetboek van Strafvordering, die ertoe strekt de bevoegdheden in te perken die bij dat artikel aan de onderzoeksrechter worden verleend wanneer het gaat om communicatiemiddelen, welke paragraaf luidt 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 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."

Artikel 12 van het voorontwerp strekt er zijnerzijds toe paragraaf 2 van artikel 18/3 van de wet van 30 november 1998 te vervangen door een bepaling waarbij wordt opgelegd dat, in de motivering van de beslissing van het diensthoofd om specifieke maatregelen aan te wenden voor het verzamelen van gegevens,[50] "in voorkomend geval, de ernstige aanwijzingen [worden opgenomen] 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."

[49] Te weten artikel 46*quinquies* en artikel 89*ter* van het Wetboek van Strafvordering.

[50] Inzonderheid die waarin is voorzien in de artikelen 18/7 en 18/8 van dezelfde wet.

dans le temps prévues à l'article 88*bis*, § 2, en projet, ne sont pas prévues par l'article 46*bis*, § 1er, alinéa 4, en projet.

Article 9

1. Si, comme l'a précisé le délégué du ministre, dans l'énumération des infractions concernées, l'article 88*bis*, § 2, 2e tiret, en projet, reproduit des dispositions existantes[49], il apparaît néanmoins qu'aux fins de refléter plus fidèlement l'intention de l'auteur de l'avant-projet, l'article 88*bis*, § 2, deuxième tiret, sera mieux rédigé comme suit:

"– Pour les autres infractions visées à l'article 90*ter*, § § 2 à 4, ou qui n'étant pas visées à cette disposition, sont commises dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal ou sont de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde (la suite comme à l'avant-projet);".

2. L'article 9 de l'avant-projet entend insérer un paragraphe 3 nouveau dans l'article 88*bis* du Code d'instruction criminelle, qui tend à limiter les pouvoirs conférés par cet article au juge d'instruction lorsque sont concernés les moyens de communication, paragraphe 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 paragraphe 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 paragraphes 1er, utilisent ses moyens de communication électronique.

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

Quant à l'article 12 de l'avant-projet, il entend remplacer le paragraphe 2 de l'article 18/3 de la loi du 30 novembre 1998 par une disposition qui, dans la motivation de la décision du dirigeant du service de recourir à des mesures spécifiques de recueil de données[50], impose que figurent "le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle".

[49] À savoir l'article 46*quinquies* et l'article 89*ter* du Code d'instruction criminelle.

[50] Notamment celles prévues aux articles 18/7 et 18/8 de la même loi.

In haar gunstig advies nr. 33/2015, op 9 september 2015 gegeven over de ontworpen tekst, merkt de Commissie voor de bescherming van de persoonlijke levenssfeer, bij de vergelijking van die twee bepalingen, "wel op dat het voorontwerp van wet de beroepsgroep van de journalisten niet heeft opgenomen in [de uitzonderingsmaatregel vervat in artikel 9 van het voorontwerp], hetgeen daarentegen wel is gebeurd in artikel 12 van het voorontwerp van wet." Bijgevolg vraagt de Commissie om "tevens de journalisten in deze uitzonderingsmaatregel op te nemen".

Het voorontwerp is niet gewijzigd ten gevolge van die opmerking. In de artikelsgewijze bespreking wordt daarvoor de volgende uitleg gegeven:

"In haar voormelde advies vraagt de Privacycommissie om journalisten op te nemen bij de beroepen die door § 3 worden beschermd. Zo'n toevoeging wordt niet nodig geacht omdat journalisten al het voordeel hebben van de bescherming die hun wordt geboden door de wet van 7 april 2005 tot bescherming van de journalistieke bronnen. De toegang tot de gegevens is maar mogelijk als de informatie als cruciaal wordt geacht voor de identificatie van en zoektocht naar de daders van misdrijven die de fysieke integriteit in gevaar brengen of om dergelijke feiten te voorkomen. Bovendien kan het journalistieke brongeheim maar worden opgeheven indien de gevraagde informatie op geen andere manier kan worden verkregen. De tussenkomst van de rechter waarborgt de naleving van deze vereisten (DOC 51-24/001, p. 13).

Overeenkomstig artikel 5 van de wet van 7 april 2005 mogen gegevens die betrekking hebben op de informatiebronnen van journalisten, niet het voorwerp uitmaken van enige opsporings- of onderzoeksmaatregel, tenzij die gegevens kunnen voorkomen dat misdrijven worden gepleegd die de fysieke integriteit van een of meer personen ernstig in het gedrang brengen, in de hierboven vermelde omstandigheden.

In de voorbereiding van de wet van 7 april 2005 wordt duidelijk gezegd: "Het spreekt vanzelf dat de journalist zijn informatie op wettige wijze moet verkregen hebben. Dit houdt in dat een journalist die zijn informatie verkreeg door middel van een misdrijf strafrechtelijk vervolgd kan worden." (DOC 51-24/001, p. 11)

Zoals bovendien eerder is gepreciseerd, weerspiegelt artikel 88*bis* hetgeen reeds bestaat in de artikelen 56*bis* en 90*octies*. Welnu, deze twee artikelen doelen enkel op advocaten of artsen."

Het geheim van de journalistieke bronnen wordt inderdaad reeds door bijzondere maatregelen beschermd wat betreft het gebruik van gegevens in dat verband door gerechtelijke instanties.

Zo bepaalt artikel 5 van de wet van 7 april 2005 "tot bescherming van de journalistieke bronnen" immers wat volgt:

"Art. 5. Gegevens die betrekking hebben op de informatiebronnen van de personen bedoeld in artikel 2, mogen niet het voorwerp uitmaken van enige opsporings- of onderzoeksmaatregel, tenzij die gegevens kunnen voorkomen dat

Comparant ces deux dispositions, dans son avis favorable n° 33/2015 donné le 9 septembre 2015 sur le texte en projet, la Commission pour la protection de la vie privée "remarque toutefois que l'avant-projet de loi n'a pas repris la catégorie professionnelle des journalistes dans [la mesure d'exception prévue à l'article 9 de l'avant-projet], ce qui était par contre le cas à l'article 12 de l'avant-projet de loi." En conséquence, la Commission demande "d'également appliquer cette mesure d'exception aux journalistes".

L'avant-projet n'a pas été modifié à la suite de cette observation. Le commentaire des articles s'en explique comme suit:

"Dans son avis précité, la Commission vie privée demande d'inclure les journalistes parmi les professions protégées par le § 3. Un tel ajout n'est pas jugé nécessaire car les journalistes bénéficient déjà de la protection qui leur est accordée par la loi du 7 avril 2005 relative à la protection des sources journalistes. L'accès aux données n'est possible que si l'information est jugée cruciale pour l'identification et la recherche des auteurs d'infractions mettant en danger l'intégrité physique ou pour éviter ce type d'infraction. En outre, le secret des sources journalistiques ne peut être levé que si l'information demandée ne peut être obtenue autrement. L'intervention du juge garantit le respect de ces exigences (DOC 51-24/001, p. 13).

En application de l'article 5 de la loi du 7 avril 2005, il ne pourra être procédé à aucune mesure d'information ou d'instruction concernant des données relatives aux sources d'information des journalistes, sauf si ces données sont susceptibles de prévenir la commission des infractions constituant une menace grave pour l'intégrité physique d'une ou de plusieurs personnes dans les conditions citées' ci-avant.

Les travaux préparatoires de la loi du 7 avril 2005 précisent que "Il va de soi que le journaliste doit avoir obtenu ses informations de manière licite. Un journaliste qui a obtenu ses informations en commettant une infraction sera donc passible de poursuites pénales" (DOC 51-24/001, p. 11).

En outre, comme précisé précédemment, l'article 88*bis* reflète ce qui existe déjà dans les articles 56*bis* et 90*octies*. Or, ces deux articles visent uniquement l'avocat ou le médecin".

Effectivement, le secret des sources des journalistes fait déjà l'objet de mesures de protection particulières en matière d'utilisation judiciaire des données y afférentes.

Ainsi, l'article 5 de la loi du 7 avril 2005 "relative à la protection des sources journalistes" dispose en effet comme suit:

"Art. 5. Il ne pourra être procédé à aucune mesure d'information ou d'instruction concernant des données relatives aux sources d'information des personnes visées à l'article 2, sauf si ces données sont susceptibles de prévenir la commission

de in artikel 4 bedoelde misdrijven worden gepleegd, en met naleving van de daarin bepaalde voorwaarden."

Aangezien die bepaling enkel betrekking heeft op opsporings- en onderzoeksmaatregelen, en dus niet op de inlichtingen- en veiligheidsmaatregelen, is het gerechtvaardigd dat in de ontworpen tekst voorzien wordt in aanvullende maatregelen tot bescherming van de bronnen tegen het verzamelen van gegevens in het kader van inlichtingen en veiligheid, zonder te voorzien in maatregelen op gerechtelijk vlak.

Artikel 10

De woorden "wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 5, vierde lid," moeten worden vervangen door de woorden "worden tevens de gegevens gevoegd bedoeld in artikel 126, § 5, vierde lid,".

De griffier, *De voorzitter,*

Colette GIGOT Pierre LIÉNARDY

des infractions visées à l'article 4, et dans le respect des conditions qui y sont définies".

Cette disposition n'ayant trait qu'aux mesures d'information et d'instruction et non pas aux mesures de renseignement et de sécurité, il se justifie que le texte en projet envisage des mesures complémentaires de protection des sources pour le recueil de données en matière de renseignement et de sécurité, sans en prévoir en matière judiciaire.

Article 10

Il convient de remplacer les mots "est joint le rapport dressé en application de l'article 126, § 5, alinéa 4," par les mots "sont jointes les données visées à l'article 126, § 5, alinéa 4,".

Le greffier, *Le président,*

Colette GIGOT Pierre LIÉNARDY

WETSONTWERP

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 58 449 van 8 december 2015 van de Raad van State;

Gelet op de raadpleging vanaf 27 oktober 2015 tot en met 6 november 2015 van het Interministerieel Comité voor Telecommunicatie en Radio-omroep en Televisie;

Gelet op het akkoord van het Overlegcomité van 25 november 2015;

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, de minister van Justitie en de minister van Defensie zijn ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen:

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid zoals bepaald in artikel 74 van de Grondwet.

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,
SALUT.

Vu les lois sur le Conseil d'État, 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 58 449 émis le 8 décembre 2015 par le Conseil d'État;

Vu la consultation du 27 octobre 2015 au 6 novembre 2015 du Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision;

Vu l'accord du Comité de concertation du 25 novembre 2015;

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, le ministre de la Justice et le ministre de la Défense sont chargés de présenter en notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Dispositions générales

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

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:

1° de bepaling onder 11° wordt vervangen als volgt:

"11° "operator": een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9; ";

2° het artikel wordt aangevuld met een bepaling onder 74° luidende als volgt:

"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. ".

Art. 3

Artikel 125, § 2, gewijzigd bij de wetten van 10 juli 2012 en 27 maart 2014, van dezelfde wet wordt opgeheven.

Art. 4

Artikel 126 van dezelfde wet wordt vervangen als volgt:

"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 operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten 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.

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

CHAPITRE 2

Modifications de la loi du 13 juin 2005 relative aux communications électroniques

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° le 11° est remplacé par ce qui suit:

"11° "opérateur": toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;";

2° l'article est complété par un 74° rédigé comme suit:

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

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

L'article 126 de la même loi est remplacé par ce qui suit:

"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 opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, 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.

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:

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

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

§ 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:

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 46*bis* en 88*bis* van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen.

2° De inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren 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 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.

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

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

§ 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° 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 46*bis* et 88*bis* du Code d'instruction criminelle et dans les conditions fixées par ces articles.

2° Les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil 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.

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.

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

de vermiste persoon in onmiddellijk gevaar is. Enkel de gegevens die zijn beoogd in paragraaf 3, de leden 1 en 2, 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 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 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd.

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.

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.

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

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf 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

trouve en danger imminent. Seules les données visées au paragraphe 3, alinéas 1 et 2, 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 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 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées.

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.

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. 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 et 3, 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.

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, sont conservées pendant douze 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, sont conservées pendant douze 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

per type van categorie bedoeld in de leden 1 tot 3 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 126/1, § 1;

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

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;

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;

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. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.

§ 5. De minister en de minister van Justitie zorgen ervoor dat statistieken inzake de bewaring van de

1 à 3 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;

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

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° 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° 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. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des

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.

Die statistieken omvatten met name:

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens 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 90*decies* 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 de oproeper

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.

Ces statistiques comprennent notamment:

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

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

3° les cas dans lesquels des demandes de données 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

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.

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.

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

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.

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.

De operatoren en aanbieders die geen van de diensten beoogd in artikel 126, § 1, verstrekken, zijn vrijgesteld van de in het derde lid, 1°, beoogde voorwaarde.

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.

De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.

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 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.

§ 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

de 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.

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.

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

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° 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.

Les opérateurs et fournisseurs qui ne fournissent aucun des services visés à l'article 126, § 1er, sont dispensés de la condition visée à l'alinéa 3, 1°.

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.

Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.

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 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. 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

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.

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.

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.

§ 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.

Verscheidene operatoren of aanbieders mogen een of meer gemeenschappelijke aangestelden voor de bescherming van de persoonsgegevens aanduiden. In dat geval moet(en) deze aangestelde(n) dezelfde opdracht uitvoeren voor elke individuele operator of aanbieder.

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.

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.

De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met de directie van de operator of de aanbieder.

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

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.

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.

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. 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.

Plusieurs opérateurs ou fournisseurs peuvent désigner un ou plusieurs préposés à la protection des données à caractère personnel communs. En pareil cas, ce ou ces préposé(s) doi(ven)t assurer la même mission pour chaque opérateur ou fournisseur individuel.

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.

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.

Le préposé doit avoir la possibilité de communiquer directement avec la direction de l'opérateur ou du fournisseur.

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

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

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

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

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.

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.

§ 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:

1° de nadere bepalingen van de aanvraag en de verstrekking van het veiligheidsadvies;

2° de vereisten waaraan de Coördinatiecel moet beantwoorden, door rekening te houden met de situatie van de operatoren en aanbieders die weinig verzoeken krijgen van de gerechtelijke overheden, die geen vestiging hebben in België of voornamelijk vanuit het buitenland handelen;

3° 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;

4° 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, desgevallend en per betrokken overheid met inbegrip van de vorm en de inhoud van het verzoek."

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

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

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

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.

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

2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en compte la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger ;

3° 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;

4° 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, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande".

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 in het eerste lid, 2°, bedoelde verrichtingen";

2° paragraaf zes wordt opgeheven.

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:

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

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

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

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

1° 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;

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.".

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° le paragraphe 6 est abrogé.

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

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

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

"§ 3*ter*. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126;

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

Art. 8

In artikel 46*bis*, § 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:

"Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf 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."

Art. 9

In artikel 88*bis* 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:

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

"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:

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

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

2° In § 1, tweede lid wordt het woord "telecommunicatiemiddel" vervangen door de woorden "elektronisch

CHAPITRE 3

Dispositions modifiant le Code d'instruction criminelle

Art. 8

A l'article 46*bis*, § 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:

"Pour des infractions qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, 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

A l'article 88*bis* 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° Au § 1er, l'alinéa 1er est remplacé comme suit:

"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° 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° Au § 1er, alinéa 2, les mots "moyen de télécommunication" sont remplacés par les mots "moyen

communicatiemiddel" en het woord "telecommunicatie" door het woord "elektronische communicatie".

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

"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."

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

"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."

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

"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."

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

"§ 2. Wat betreft de toepassing van de maatregel bedoeld in § 1 op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

— Voor een strafbaar feit bedoeld in Titel Iter van Boek II van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift.

— Voor andere strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, of die gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of die een gevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kunnen hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

— Voor andere strafbare feiten niet bedoeld in de vorige twee onderdelen, kan de onderzoeksrechter de gegevens bedoeld in § 1, eerste lid, die op basis van

de communication électronique" et les mots "de la télécommunication" par les mots "de la communication électronique".

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

"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° § 1er, alinéa 4, est remplacé par:

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

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

"§ 2. Pour ce qui concerne l'application de la mesure visée au § 1er aux données de trafic ou de localisation conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:

— Pour une infraction visée au Titre Iter du Livre II du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance.

— Pour les autres infractions visées à l'article 90*ter*, §§ 2 à 4, ou qui sont commises dans le cadre d'une organisation criminelle visée à l'article 324*bis* 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 pour une période de neuf mois préalable à l'ordonnance.

— Pour d'autres infractions non visées par les deux points précédents, le juge d'instruction ne peut requérir les données visées au § 1er, alinéa 1er, qui

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."

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 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 90*decies* 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. ".

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."

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 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 90*decies* 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."

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:

“De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die zij leveren.”

3° Er wordt een vierde lid ingevoegd, luidend als volgt:

“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.”

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:

1° Er wordt een § 2 ingevoegd, luidend als volgt:

“§ 2. De beslissing van het diensthoofd vermeldt:

1° de aard van de specifieke methode;

2° naargelang het geval, de natuurlijke perso(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 dreiging 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°;

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:

“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° Un quatrième alinéa est inséré, libellé comme suit:

“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

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° Un § 2 est inséré, libellé comme suit:

“§ 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° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen;

7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode;

8° in voorkomend geval, de samenloop met een 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 dreiging;

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."

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° tot 3°, 5° en 7°.".

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

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

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

"§ 8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging 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."

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

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

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

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."

Art. 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 wijzigingen aangebracht:

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

"De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of 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."

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

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

"§ 2. Wat betreft de toepassing van de methode bedoeld in § 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

1°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing.

2°) Voor een potentiële dreiging zoals bedoeld in artikel 18/1, andere dan deze bedoeld in 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing.

Art. 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:

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

"Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de 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 adressées ou ont été adressées;

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

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

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

"§ 2. Pour ce qui concerne l'application de la méthode visée au § 1er aux données conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:

1°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut requérir les données que pour une période de six mois préalable à la décision.

2°) Pour une menace potentielle autre que celles visées sous 1° et 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision.

3°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing.

4° § 2 wordt vernummerd tot § 4.

Gegeven te Ciergnon, 26 december 2015

FILIP

Van Koningswege:

De minister van Justitie,

Koen GEENS

De minister van Digitale Agenda, Telecommunicatie en Post,

Alexander DE CROO

De minister van Defensie,

Steven VANDEPUT

3°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision.

4° Le § 2 est renuméroté en § 4.

Donné à Ciergnon, le 26 décembre 2015

PHILIPPE

Par le Roi:

Le ministre de la Justice,

Koen GEENS

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

Alexander DE CROO

Le ministre de la Défense,

Steven VANDEPUT

BIJLAGE

ANNEXE

Ontwerp van wet betreffende
de bewaring van gegevens in de elektronische-communicatiesector

BASISTEKST	BASISTEKST AANGEPAST AAN HET WETSONTWERP	Artikel van het wetsontwerp
	HOOFDSTUK 2. - Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie	
Artikel 2. Voor de toepassing van deze wet wordt verstaan onder: […] 11° " operator " : een persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9; […]	**Artikel 2.** Voor de toepassing van deze wet wordt verstaan onder: […] ***11° "operator" : een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9***; […] ***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.***	Artikel 2 wetsontwerp
Artikel 125. § 2. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels en de middelen die moeten worden ingezet om het identificeren, het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van elektronische communicatie mogelijk te maken.	[…]	Artikel 3 wetsontwerp
Artikel 126. § 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning 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 voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de	***Artikel 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 operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken de in paragraaf 3***	Artikel 4 wetsontwerp

beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst , evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. § 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut. De operatoren zorgen ervoor dat de in §1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.	***beoogde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.*** ***Dit artikel heeft geen betrekking op de inhoud van de communicatie.*** ***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:*** ***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*** ***2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.*** ***§ 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:*** ***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.*** ***2° De inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren 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 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.*** ***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 en 2, 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 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. ***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.*** ***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.*** ***§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin de leden 2 en 3 specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.*** ***De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.*** ***De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf 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 3 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 126/1, § 1;*** ***4° de gegevens op het grondgebied van de Europese Unie te bewaren;*** ***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; ***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;*** ***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. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.*** ***§ 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.*** ***Die statistieken omvatten met name:*** ***1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens 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.***	
	Artikel 126/1. § 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	Artikel 5 wetsontwerp

	artikelen 122, 123 en 126, de identificatiegegevens van de oproeper krachtens artikel 107, § 2, eerste lid, of de gegevens die kunnen vereist zijn krachtens de artikelen 46bis, 88bis en 90ter 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. ***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.*** ***Om deel uit te maken van de Coördinatiecel dient voorafgaand te worden voldaan aan de volgende cumulatieve voorwaarden:*** ***1° Het voorwerp hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies conform artikel 22quinquies 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.*** ***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.*** ***De operatoren en aanbieders die geen van de diensten beoogd in artikel 126, § 1, verstrekken, zijn vrijgesteld van de in het derde lid, 1°, beoogde voorwaarde.*** ***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. ***De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.*** ***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 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.*** ***§ 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.*** ***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.*** ***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. ***§ 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.*** ***Verscheidene operatoren of aanbieders mogen een of meer gemeenschappelijke aangestelden voor de bescherming van de persoonsgegevens aanduiden. In dat geval moet(en) deze aangestelde(n) dezelfde opdracht uitvoeren voor elke individuele operator of aanbieder.*** ***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.*** ***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.*** ***De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met de directie van de operator of de aanbieder.***	

	In het bijzonder zorgt de aangestelde voor de gegevensbescherming ervoor dat: ***1° de behandelingen door de Coördinatiecel worden uitgevoerd conform de wet;*** ***2° de aanbieder of de operator enkel die gegevens verzamelt en bewaart die hij wettelijk mag bewaren;*** ***3° enkel de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens;*** ***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.*** ***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.*** ***§ 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:*** ***1° de nadere bepalingen van de aanvraag en de verstrekking van het veiligheidsadvies;*** ***2° de vereisten waaraan de Coördinatiecel moet beantwoorden, door rekening te houden met de situatie van de operatoren en aanbieders die***	

	weinig verzoeken krijgen van de gerechtelijke overheden, die geen vestiging hebben in België of voornamelijk vanuit het buitenland handelen; ***3° 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;*** ***4° 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, desgevallend en per betrokken overheid met inbegrip van de vorm en de inhoud van het verzoek.***	
Artikel 127. § 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren of aan de eindgebruikers worden opgelegd om : 1° in het kader van een noodoproep de oproeplijn te kunnen identificeren; 2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	**Artikel 127.** § 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren***, aan de aanbieders beoogd in artikel 126, § 1, eerste lid,*** of aan de eindgebruikers worden opgelegd om : 1° in het kader van een noodoproep de oproeplijn te kunnen identificeren; 2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	Artikel 6 wetsontwerp

De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.	De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren ***en de aanbieders beoogd in artikel 126, § 1, eerste lid,*** aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.	
§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.	§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.	
§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.	§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.	
§ 4. Indien een operator binnen de door de Koning vastgestelde termijn niet voldoet aan de hem opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.	§ 4. Indien een operator binnen de door de Koning vastgestelde termijn niet voldoet aan de hem opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.	
§ 5. De operatoren sluiten de eindgebruikers die binnen de door de Koning vastgestelde termijn niet voldoen aan de hen opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting. Indien een operator binnen de door de Koning vastgestelde termijn niet overgaat tot de afsluiting van de	§ 5. De operatoren sluiten de eindgebruikers die binnen de door de Koning vastgestelde termijn niet voldoen aan de hen opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting. Indien een operator binnen de door de Koning vastgestelde termijn niet overgaat tot de afsluiting van de	

eindgebruikers die niet voldoen aan de hen opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de eindgebruiker niet heeft voldaan aan de hem opgelegde maatregelen, te verstrekken totdat de identificatie van de oproeper mogelijk is gemaakt. § 6. Elke operator zet een interne procedure op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op grond van paragraaf 1. Hij verstrekt op verzoek aan het Instituut gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en zijn antwoord.	eindgebruikers die niet voldoen aan de hen opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de eindgebruiker niet heeft voldaan aan de hem opgelegde maatregelen, te verstrekken totdat de identificatie van de oproeper mogelijk is gemaakt. […]	
Artikel 145. § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 114, 124, 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47 en 127 genomen besluiten overtreedt. § 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt. § 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft : 1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	**Artikel 145.** § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 114, 124, ***126, 126/1,*** 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47***, 126, 126/1*** en 127 genomen besluiten overtreedt. § 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt. § 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft : 1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	Artikel 7 wetsontwerp

2° (opgeheven) 3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan. § 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan. § 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	2° (opgeheven) 3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan. § 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan. ***§ 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:*** ***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;*** ***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.*** § 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	

	HOOFDSTUK 3. – Wijziging van het Wetboek van Strafvordering	
Artikel 46bis	**Artikel 46bis**	Artikel 8 wetsontwerp
§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing, door zo nodig de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst of van een politiedienst aangewezen door de Koning te vorderen, overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de operator of van de dienstenverstrekker tot: 1° de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel; 2° de identificatie van de elektronische ncommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.	§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing, door zo nodig de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst of van een politiedienst aangewezen door de Koning te vorderen, overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de operator of van de dienstenverstrekker tot: 1° de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel; 2° de identificatie van de elektronische ncommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.	
De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.	De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.	
In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing deze gegevens opvorderen. De officier van gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen vierentwintig uur mee aan de procureur des Konings en motiveert tevens de	In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing deze gegevens opvorderen. De officier van gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen vierentwintig uur mee aan de procureur des Konings en motiveert tevens de	

uiterst dringende noodzakelijkheid.	uiterst dringende noodzakelijkheid. **<u>Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf 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.</u>**	
§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd binnen een termijn te bepalen door de Koning, op het voorstel van de Minister van Justitie en de Minister bevoegd voor Telecommunicatie.	§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd binnen een termijn te bepalen door de Koning, op het voorstel van de Minister van Justitie en de Minister bevoegd voor Telecommunicatie.	
De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie en van de minister die bevoegd is voor Telecommunicatie, de technische voorwaarden voor de toegang tot de in § 1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.	De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie en van de minister die bevoegd is voor Telecommunicatie, de technische voorwaarden voor de toegang tot de in § 1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.	
Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	
Weigering de gegevens mee te delen, wordt gestraft met geldboete van	Weigering de gegevens mee te delen, wordt gestraft met geldboete van	

zesentwintig euro tot tienduizend euro.	zesentwintig euro tot tienduizend euro.	
Artikel 88bis	**Artikel 88bis**	Artikel 9 wetsontwerp
§ 1. Wanneer de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van telecommunicatie of het lokaliseren van de oorsprong of de bestemming van telecommunicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij, zo nodig door daartoe de medewerking van de operator van een telecommunicatienetwerk of van de verstrekker van een telecommunicatiedienst te vorderen: 1° de oproepgegevens doen opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan; 2° de oorsprong of de bestemming van telecommunicatie laten lokaliseren.	§ 1. **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:** **1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;** **2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren**	
In de gevallen bepaald in het eerste lid wordt voor ieder telecommunicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de telecommunicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.	In de gevallen bepaald in het eerste lid wordt voor ieder **elektronisch communicatiemiddel** waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de **elektronische communicatie** wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.	
De onderzoeksrechter vermeldt de feitelijke omstandigheden van de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij	**De onderzoeksrechter doet in een gemotiveerd bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de**	

meedeelt aan de procureur des Konings.	**proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.**	
Hij vermeldt ook de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing.	**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.**	
In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter. Indien het echter het in artikel 347bis of 470 van het Strafwetboek bedoelde strafbare feit betreft, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.	In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter. Indien het echter het in artikel 347bis of 470 van het Strafwetboek bedoelde strafbare feit betreft, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.	
De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.	De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.	
	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	
	§ 2. Wat betreft de toepassing van de maatregel bedoeld in § 1 op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische	

	communicatie, zijn de volgende bepalingen van toepassing: - **Voor een strafbaar feit bedoeld in Titel Iter van Boek II van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift.** - **Voor andere strafbare feiten 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 vijf jaar of een zwaardere straf tot gevolg kunnen hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;** - **Voor andere strafbare feiten niet bedoeld in de vorige twee onderdelen, 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.** **§ 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 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.	
§2. Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst deelt de gegevens waarom verzocht werd mee binnen een termijn te bepalen door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig frank tot tienduizend frank (lees euro).	**§4. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst** deelt de gegevens waarom verzocht werd mee binnen een termijn te bepalen door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig frank tot tienduizend frank (lees euro).	
Artikel 90decies De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.	**Article 90decies** De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.	Artikel 10 wetsontwerp

Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter. Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven. Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.	Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter. Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven. Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. **<u>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.</u>**	
	HOOFDSTUK 4. –Wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten	
Artikel 13. In het raam van hun opdrachten kunnen de inlichtingen- en	**Artikel 13.** In het raam van hun opdrachten kunnen de inlichtingen- en	Artikel 11 wetsontwerp

veiligheidsdiensten inlichtingen en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten. De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien. De inlichtingen- en veiligheidsdiensten die gebruik maken van de methoden voor het verzamelen van gegevens als bedoeld in de onderafdelingen 2 en 2bis dienen te waken over de veiligheid van de gegevens die betrekking hebben op menselijke bronnen en over de informatie die zij meedelen.	veiligheidsdiensten ~~**inlichtingen**~~ **informatie** en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten. De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien. ~~**De inlichtingen- en veiligheidsdiensten die gebruik maken van de methoden voor het verzamelen van gegevens als bedoeld in de onderafdelingen 2 en 2bis dienen te waken over de veiligheid van de gegevens die betrekking hebben op menselijke bronnen en over de informatie die zij meedelen.**~~ **De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die zij leveren.** **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.**	
Artikel 18/3. §1. Rekening houdend met een potentiële bedreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die	**Article 18/3.** §1. Rekening houdend met een potentiële bedreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die	Artikel 12 wetsontwerp

nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële bedreiging waarvoor ze wordt aangewend.	nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële bedreiging waarvoor ze wordt aangewend.	
De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.	De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.	
De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen-en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd.	~~De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd.~~	
De inlichtingenofficier die is aangesteld om de specifieke methode voor het verzamelen van gegevens aan te wenden, informeert het diensthoofd regelmatig over de uitvoering van deze methode.	~~De inlichtingenofficier die is aangesteld om de specifieke methode voor het verzamelen van gegevens aan te wenden, informeert het diensthoofd regelmatig over de uitvoering van deze methode.~~	
§2. Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.	**§2.** ~~Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.~~	
De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.	~~De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.~~	
Zij kunnen daartoe de plaatsen betreden	~~Zij kunnen daartoe de plaatsen betreden~~	

waar de gegevens betreffende de specifieke methode door de inlichtingen- en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	~~waar de gegevens betreffende de specifieke methode door de inlichtingen en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.~~	
De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen-en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.	~~De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.~~	
De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.	~~De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.~~ **De beslissing van het diensthoofd vermeldt:** **1° de aard van de specifieke methode;** **2° naargelang het geval, de natuurlijke perso(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 dreiging 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 Commissie;** **6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen ;** **7° in voorkomend geval, het technisch**	

	middel dat gebruikt wordt bij de aanwending van de specifieke methode; **8° in voorkomend geval, de samenloop met een 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 dreiging;** **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.**	
§3. De lijsten bedoeld in § 2 bevatten de volgende gegevens : 1° de aard van de specifieke methode voor het verzamelen van gegevens; 2° de graad van de ernst van de bedreiging die de specifieke methode voor het verzamelen van gegevens wettigt; 3° naargelang het geval, de natuurlijke of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode voor het verzamelen van gegevens; 4° het technische middel dat gebruikt wordt om de specifieke methode voor het verzamelen van gegevens aan te wenden; 5° de periode tijdens welke de specifieke methode voor het verzamelen van gegevens kan worden uitgevoerd te rekenen van de beslissing.	**§3. ~~De lijsten bedoeld in § 2 bevatten de volgende gegevens :~~** **~~1° de aard van de specifieke methode voor het verzamelen van gegevens;~~** **~~2° de graad van de ernst van de bedreiging die de specifieke methode voor het verzamelen van gegevens wettigt;~~** **~~3° naargelang het geval, de natuurlijke of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode voor het verzamelen van gegevens;~~** **~~4° het technische middel dat gebruikt wordt om de specifieke methode voor het verzamelen van gegevens aan te wenden;~~** **~~5° de periode tijdens welke de specifieke methode voor het verzamelen van gegevens kan worden uitgevoerd te rekenen van de beslissing.~~** **Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.**	

	Deze lijsten bevatten de gegevens bedoeld in §2, 1° tot 3°, 5° en 7°.	
§4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.	§4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.	
	§5. De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen-en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd.	
	§6. De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.	
	Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen-en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	
	De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de	

	commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen-en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is. **De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.** **§7. De inlichtingenofficier die is aangesteld ~~om de specifieke methode voor het verzamelen van gegevens aan te wenden~~ om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen, informeert het diensthoofd regelmatig over de uitvoering van deze methode.** **§8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging 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.**	
Artikel 18/8. §1. Wanneer dit een belang vertoont voor de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, zo nodig door daartoe de technische medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot : 1° het opsporen van de oproepgegevens van elektronische communicatiemiddelen van waaruit of waarnaar oproepen worden of werden gericht;	**Article 18/8. §1. ~~Wanneer dit een belang vertoont voor de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, zo nodig door daartoe de technische medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot :~~** **~~1° het opsporen van de oproepgegevens van elektronische communicatiemiddelen van waaruit of waarnaar oproepen worden of werden gericht;~~**	Artikel 13 wetsontwerp

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.	~~**2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.**~~ **De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:** **1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;** **2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.**	
In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.	In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de ~~**oproepgegevens**~~ **verkeersgegevens** worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.	
De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	
§2. In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze	**§2.** ~~**In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze**~~	

mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd.	~~**mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd.**~~	
De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	~~**De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.**~~ **Wat betreft de toepassing van de methode bedoeld in § 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:** **1°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing.** **2°) Voor een potentiële dreiging zoals bedoeld in artikel 18/1, andere dan deze bedoeld in 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing.** **3°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing.**	
§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de	§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de	

gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie. Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.	gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie. Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro. **§4. In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd.** **De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.**	

Projet de loi relative à
la conservation des données dans le secteur des communications électroniques

TEXTE DE BASE	TEXTE DE BASE ADAPTE AU PROJET	Article du projet de loi
	CHAPITRE 2. – Modifications de la loi du 13 juin 2005 relative aux communications électroniques	
Article 2. Pour l'application de la présente loi, il faut entendre par : […] 11° " opérateur " : toute personne ayant introduit une notification conformément à l'article 9; […]	**Article 2.** Les modifications suivantes sont apportées : […] ***11° "opérateur" : toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;*** […] ***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.***	Article 2 du projet
Article 125. § 2. Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en oeuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques.	[…]	Article 3 du projet
Article 126. § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation	***Article 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 opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, 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.***	Article 4 du projet

malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. § 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut. Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique.	***Le présent article ne porte pas sur le contenu des communications.*** ***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° 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° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.*** ***§ 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° 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° Les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil 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.*** ***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.*** ***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 et 2, 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 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.*** ***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. ***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. 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 et 3, 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.*** ***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, sont conservées pendant douze 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, sont conservées pendant douze 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 3 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 ;*** ***4° conservent les données sur le territoire de l'Union européenne ;*** ***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° 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° 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. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal. ***§ 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.*** ***Ces statistiques comprennent notamment :*** ***1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;*** ***2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;*** ***3° les cas dans lesquels des demandes de données 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 90decies 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.***	
	Article 126/1. § 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 l'appelant en vertu de l'article 107, § 2, alinéa 1er ou les données qui peuvent être requises en vertu des articles 46bis, 88bis et 90ter 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. ***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.*** ***Afin de faire partie de la Cellule coordination, il faut au préalable répondre aux conditions cumulatives suivantes :*** ***1° Avoir fait l'objet d'un avis de sécurité positif et non périmé conformément à l'article 22quinquies 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.***	Article 5 du projet

	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. ***Les opérateurs et fournisseurs qui ne fournissent aucun des services visés à l'article 126, § 1er, sont dispensés de la condition visée à l'alinéa 3, 1°.*** ***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.*** ***Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.*** ***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 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. 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.*** ***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. ***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. 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.*** ***Plusieurs opérateurs ou fournisseurs peuvent désigner un ou plusieurs préposés à la protection des données à caractère personnel communs. En pareil cas, ce ou ces préposé(s) doi(ven)t assurer la même mission pour chaque opérateur ou fournisseur individuel.*** ***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.*** ***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. ***Le préposé doit avoir la possibilité de communiquer directement avec la direction de l'opérateur ou du fournisseur.*** ***Le préposé à la protection des données veille à ce que :*** ***1° les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi ;*** ***2° le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver ;*** ***3° seules les autorités légalement autorisées aient accès aux données conservées ;*** ***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.*** ***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. 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° les modalités de la demande et de l'octroi de l'avis de sécurité ;*** ***2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en***	

	compte ***la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger ;*** ***3° 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 ;*** ***4° 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, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande ».***	
Article 127. § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre : 1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence; 2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner	**Article 127.** § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, ***aux fournisseurs visés à l'article 126, § 1er, alinéa 1er,*** ou aux utilisateurs finals, en vue de permettre : 1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence; 2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs ***et des fournisseurs visés à l'article 126, § 1er, alinéa 1er***, aux opérations visées à l'alinéa 1er, 2° ainsi que	Article 6 du projet

suite aux mesures imposées.	le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.	
§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	
§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.	§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.	
§ 4. Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.	§ 4. Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.	
§ 5. Les opérateurs déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion. Si un opérateur ne déconnecte pas les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible.	§ 5. Les opérateurs déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion. Si un opérateur ne déconnecte pas les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible.	
§ 6. Chaque opérateur établit, sur la base du paragraphe 1er, une procédure interne permettant de répondre aux demandes d'accès 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.		
Article 145. § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 114, 124, 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47 et 127. § 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16. § 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement : 1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite; 2° (abroge) 3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci. § 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la	**Article 145.** § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 114, 124, ***126, 126/1,*** 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, ***126, 126/1*** et 127. § 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16. § 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement : 1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite; 2° (abroge) 3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci. § 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la	Article 7 du projet

personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.	personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci. ***§ 3ter. Est puni d'une amende de 50 euros à 50.000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :*** ***1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126 ;*** ***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.***	
§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.	§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.	
	CHAPITRE 3. – Dispositions modifiant le Code d'instruction criminelle	
<u>Article 46bis</u> § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, en requérant au besoin le concours de l'opérateur d'une réseau de communication électronique ou d'un fournisseur d'un service de communication électronique ou d'un service de police désigné par le Roi, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients	**<u>Article 46bis</u>** § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, en requérant au besoin le concours de l'opérateur d'une réseau de communication électronique ou d'un fournisseur d'un service de communication électronique ou d'un service de police désigné par le Roi, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients	Article 8 du projet

de l'opérateur ou du fournisseur de service à : 1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilise; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence. §2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications.	de l'opérateur ou du fournisseur de service à : 1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilise; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence. **Pour des infractions qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées au premier alinéa que pour une période de six mois préalable à sa décision.** §2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications.	

Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Le refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros.	Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Le refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros.	
Article 88bis 1er. Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication : 1° au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés; 2° a la localisation de l'origine ou de la destination de télécommunications.	**Article 88bis** 1er. **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° 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.**	Article 9 du projet

Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisé, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal.	Dans les cas visés à l'alinéa 1er, pour **moyen de communication électronique** dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisé, le jour, l'heure, la durée et, si nécessaire, le lieu de **la communication électronique** sont indiqués et consignés dans un procès-verbal.	
Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi.	**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.**	
Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement.	**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.**	
En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction. S'il s'agit toutefois de l'infraction visée à l'article 347bis ou 470 du Code pénal, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction soit nécessaire.	En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction. S'il s'agit toutefois de l'infraction visée à l'article 347bis ou 470 du Code pénal, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction soit nécessaire.	
Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.	Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.	

	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. **§ 2. Pour ce qui concerne l'application de la mesure visée au § 1er aux données de trafic ou de localisation conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:** - **Pour une infraction visée au Titre Iter du Livre II du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance.** - **Pour les autres infractions 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 pour une période de neuf mois préalable à l'ordonnance.** - **Pour d'autres infractions non visées par les deux points précédents, 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.** **§ 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 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.**	
§ 2. Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication communique les informations qui ont été demandées dans un délai a fixer par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les Télécommunications, est punie d'une amende de vingt-six francs (lire euros) à dix mille francs (lire euros).	**§4. 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** communique les informations qui ont été demandées dans un délai a fixer par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les Télécommunications, est punie d'une amende de vingt-six francs (lire euros) à dix mille francs (lire euros).	
Article 90decies Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.	**Article 90decies** Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.	Article 10 du projet

Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus. Il fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter. Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés.	Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus. Il fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter. Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés. **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	
Article 13. Dans le cadre de leurs missions, ils peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux	**Article 13.** Dans le cadre de leurs missions, ils peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux	Article 11 du projet

exigences qui en découlent. Les services de renseignement et de sécurité qui ont recours aux méthodes de recueil de données visées aux sous-sections 2 et 2bis doivent veiller à la sécurité des données ayant trait aux sources humaines et aux informations qu'elles communiquent.	exigences qui en découlent. ~~**Les services de renseignement et de sécurité qui ont recours aux méthodes de recueil de données visées aux sous-sections 2 et 2bis doivent veiller à la sécurité des données ayant trait aux sources humaines et aux informations qu'elles communiquent.**~~ **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.** **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.**	
Article 18/3. §1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en oeuvre compte tenu de la menace potentielle visée à l'article 18/1, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en oeuvre. La méthode spécifique ne peut être mise en oeuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission. Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition	**Article 18/3.** §1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en oeuvre compte tenu de la menace potentielle visée à l'article 18/1, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en oeuvre. La méthode spécifique ne peut être mise en oeuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission. ~~**Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la**~~	Article 12 du projet

que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.	~~condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.~~	
L'officier de renseignement désigné pour mettre en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.	~~L'officier de renseignement désigné pour mettre en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.~~	
§2. Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.	**§2.** ~~Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.~~	
Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.	~~Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.~~	
Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.	~~Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.~~	
Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.	~~Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.~~	
La commission notifie de sa propre initiative et sans délai sa décision au	~~La commission notifie de sa propre initiative et sans délai sa décision au~~	

Comité permanent R.	~~**Comité permanent R.**~~ **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 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.**	
§3. Les listes visées au § 2 comprennent les données suivantes : 1° la nature de la méthode spécifique de recueil de données; 2° le degré de gravité de la menace qui justifie la méthode spécifique de recueil de données;	**§3.** ~~**Les listes visées au § 2 comprennent les données suivantes :**~~ ~~**1° la nature de la méthode spécifique de recueil de données;**~~ ~~**2° le degré de gravité de la menace qui justifie la méthode spécifique de recueil de données;**~~	

3° 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 de recueil de données; 4° le moyen technique employé pour mettre en oeuvre la méthode spécifique de recueil des données; 5° la période durant laquelle la méthode spécifique de recueil de données peut être mise en oeuvre à compter de la décision.	~~**3° 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 de recueil de données;**~~ ~~**4° le moyen technique employé pour mettre en oeuvre la méthode spécifique de recueil des données;**~~ ~~**5° la période durant laquelle la méthode spécifique de recueil de données peut être mise en oeuvre à compter de la décision.**~~ **Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.** **Ces listes comprennent les données visées au §2, 1° à 3°, 5° et 7°.**	
§4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er.	§4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er. **§5. Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.** **§6. Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.** **Ils peuvent, à cet effet, pénétrer dans les**	

	lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service. **Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.** **La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.** **§7. L'officier de renseignement désigné pour ~~mettre~~ le suivi de la mise en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.** **§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 oeuvre, ou quand il a été constaté une illégalité. Il informe dès que possible la commission de sa décision.**	
Article 18/8. §1er. Lorsque cela présente un intérêt pour l'exercice des missions, le dirigeant du service peut, par une décision écrite, procéder ou faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques :	**Article 18/8. §1er. ~~Lorsque cela présente un intérêt pour l'exercice des missions, le dirigeant du service peut, par une décision écrite, procéder ou faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques :~~**	Article 13 du projet

1° au repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;	~~**1° au repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;**~~	
2° à la localisation de l'origine ou de la destination de communications électroniques.	~~**2° à la localisation de l'origine ou de la destination de communications électroniques.**~~ **Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de 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 adressées ou ont été adressées ;** **2° à la localisation de l'origine ou de la destination de communications électroniques.**	
Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les données d'appel sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.	Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les ~~**données d'appel**~~ **données de trafic** sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.	
La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	
§2. En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et préalable	~~***§2. En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et***~~	

du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service. La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	~~**préalable du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service.**~~ ~~**La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.**~~ **Pour ce qui concerne l'application de la méthode visée au § 1er aux données conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent :** **1°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut requérir les données que pour une période de six mois préalable à la décision.** **2°) Pour une menace potentielle autre que celles visées sous 1° et 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision.** **3°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision.**	
§3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les Communications électroniques dans ses	*§3.* Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les Communications électroniques dans ses	

attributions. Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à dix mille euros.	attributions. Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à dix mille euros. **§4. En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et préalable du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service.** **La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.**	

BIJLAGE **ANNEXE**

Ontwerp van wet betreffende
de bewaring van gegevens in de elektronische-communicatiesector

BASISTEKST	BASISTEKST AANGEPAST AAN HET WETSONTWERP	Artikel van het wetsontwerp
	HOOFDSTUK 2. - Wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie	
Artikel 2. Voor de toepassing van deze wet wordt verstaan onder: […] 11° " operator " : een persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9; […]	**Artikel 2.** Voor de toepassing van deze wet wordt verstaan onder: […] ***11° "operator" : een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9***; […] ***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.***	Artikel 2 wetsontwerp
Artikel 125. § 2. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels en de middelen die moeten worden ingezet om het identificeren, het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van elektronische communicatie mogelijk te maken.	[…]	Artikel 3 wetsontwerp
Artikel 126. § 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning 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 voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de	***Artikel 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 operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken de in paragraaf 3***	Artikel 4 wetsontwerp

beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst , evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. § 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut. De operatoren zorgen ervoor dat de in §1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.	***beoogde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.*** ***Dit artikel heeft geen betrekking op de inhoud van de communicatie.*** ***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:*** ***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*** ***2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.*** ***§ 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:*** ***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.*** ***2° De inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren 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 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.*** ***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 en 2, 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 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. ***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.*** ***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.*** ***§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin de leden 2 en 3 specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.*** ***De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.*** ***De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf 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 3 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 126/1, § 1;*** ***4° de gegevens op het grondgebied van de Europese Unie te bewaren;*** ***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; ***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;*** ***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. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.*** ***§ 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.*** ***Die statistieken omvatten met name:*** ***1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens 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.***	
	Artikel 126/1. § 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	Artikel 5 wetsontwerp

	identificatiegegevens van de oproeper krachtens artikel 107, § 2, eerste lid, of de gegevens die kunnen vereist zijn krachtens de artikelen 46bis, 88bis en 90ter 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. ***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.*** ***Om deel uit te maken van de Coördinatiecel dient voorafgaand te worden voldaan aan de volgende cumulatieve voorwaarden:*** ***1° Het voorwerp hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies conform artikel 22quinquies 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.*** ***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.*** ***De operatoren en aanbieders die geen van de diensten beoogd in artikel 126, § 1, verstrekken, zijn vrijgesteld van de in het derde lid, 1°, beoogde voorwaarde.*** ***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. ***De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.*** ***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 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.*** ***§ 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.*** ***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.*** ***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. ***§ 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.*** ***Verscheidene operatoren of aanbieders mogen een of meer gemeenschappelijke aangestelden voor de bescherming van de persoonsgegevens aanduiden. In dat geval moet(en) deze aangestelde(n) dezelfde opdracht uitvoeren voor elke individuele operator of aanbieder.*** ***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.*** ***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.*** ***De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met de directie van de operator of de aanbieder.*** ***In het bijzonder zorgt de aangestelde***	

	voor de gegevensbescherming ervoor dat: ***1° de behandelingen door de Coördinatiecel worden uitgevoerd conform de wet;*** ***2° de aanbieder of de operator enkel die gegevens verzamelt en bewaart die hij wettelijk mag bewaren;*** ***3° enkel de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens;*** ***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.*** ***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.*** ***§ 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:*** ***1° de nadere bepalingen van de aanvraag en de verstrekking van het veiligheidsadvies;*** ***2° de vereisten waaraan de Coördinatiecel moet beantwoorden, door rekening te houden met de situatie van de operatoren en aanbieders die weinig verzoeken krijgen van de***	

	gerechtelijke overheden, die geen vestiging hebben in België of voornamelijk vanuit het buitenland handelen; ***3° 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;*** ***4° 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, desgevallend en per betrokken overheid met inbegrip van de vorm en de inhoud van het verzoek.***	
Artikel 127. § 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren of aan de eindgebruikers worden opgelegd om : 1° in het kader van een noodoproep de oproeplijn te kunnen identificeren; 2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	**Artikel 127.** § 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren***, aan de aanbieders beoogd in artikel 126, § 1, eerste lid,*** of aan de eindgebruikers worden opgelegd om : 1° in het kader van een noodoproep de oproeplijn te kunnen identificeren; 2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	Artikel 6 wetsontwerp

De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.	De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren ***en de aanbieders beoogd in artikel 126, § 1, eerste lid,*** aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.	
§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.	§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.	
§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.	§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.	
§ 4. Indien een operator binnen de door de Koning vastgestelde termijn niet voldoet aan de hem opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.	§ 4. Indien een operator binnen de door de Koning vastgestelde termijn niet voldoet aan de hem opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.	
§ 5. De operatoren sluiten de eindgebruikers die binnen de door de Koning vastgestelde termijn niet voldoen aan de hen opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting. Indien een operator binnen de door de Koning vastgestelde termijn niet overgaat tot de afsluiting van de	§ 5. De operatoren sluiten de eindgebruikers die binnen de door de Koning vastgestelde termijn niet voldoen aan de hen opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting. Indien een operator binnen de door de Koning vastgestelde termijn niet overgaat tot de afsluiting van de	

eindgebruikers die niet voldoen aan de hen opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de eindgebruiker niet heeft voldaan aan de hem opgelegde maatregelen, te verstrekken totdat de identificatie van de oproeper mogelijk is gemaakt. § 6. Elke operator zet een interne procedure op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op grond van paragraaf 1. Hij verstrekt op verzoek aan het Instituut gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en zijn antwoord.	eindgebruikers die niet voldoen aan de hen opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de eindgebruiker niet heeft voldaan aan de hem opgelegde maatregelen, te verstrekken totdat de identificatie van de oproeper mogelijk is gemaakt. […]	
Artikel 145. § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 114, 124, 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47 en 127 genomen besluiten overtreedt. § 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt. § 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft : 1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	**Artikel 145.** § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 114, 124, ***126, 126/1,*** 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47***, 126, 126/1*** en 127 genomen besluiten overtreedt. § 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt. § 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft : 1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	Artikel 7 wetsontwerp

2° (opgeheven) 3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan. § 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan. § 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	2° (opgeheven) 3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan. § 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan. ***§ 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:*** ***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;*** ***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.*** § 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	

	HOOFDSTUK 3. – Wijziging van het Wetboek van Strafvordering	
<u>Artikel 46bis</u>	**<u>Artikel 46bis</u>**	Artikel 8 wetsontwerp
§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing, door zo nodig de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst of van een politiedienst aangewezen door de Koning te vorderen, overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de operator of van de dienstenverstrekker tot:	§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing, door zo nodig de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst of van een politiedienst aangewezen door de Koning te vorderen, overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de operator of van de dienstenverstrekker tot:	
1° de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;	1° de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;	
2° de identificatie van de elektronische ncommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.	2° de identificatie van de elektronische ncommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.	
De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.	De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.	
In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing deze gegevens opvorderen. De officier van gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen	In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing deze gegevens opvorderen. De officier van gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen	

vierentwintig uur mee aan de procureur des Konings en motiveert tevens de uiterst dringende noodzakelijkheid.	vierentwintig uur mee aan de procureur des Konings en motiveert tevens de uiterst dringende noodzakelijkheid. **<u>Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf 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.</u>**	
§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd binnen een termijn te bepalen door de Koning, op het voorstel van de Minister van Justitie en de Minister bevoegd voor Telecommunicatie.	§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd binnen een termijn te bepalen door de Koning, op het voorstel van de Minister van Justitie en de Minister bevoegd voor Telecommunicatie.	
De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie en van de minister die bevoegd is voor Telecommunicatie, de technische voorwaarden voor de toegang tot de in § 1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.	De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie en van de minister die bevoegd is voor Telecommunicatie, de technische voorwaarden voor de toegang tot de in § 1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.	
Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	

Weigering de gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.	Weigering de gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.	
Artikel 88bis	**Artikel 88bis**	Artikel 9 wetsontwerp
§ 1. Wanneer de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van telecommunicatie of het lokaliseren van de oorsprong of de bestemming van telecommunicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij, zo nodig door daartoe de medewerking van de operator van een telecommunicatienetwerk of van de verstrekker van een telecommunicatiedienst te vorderen: 1° de oproepgegevens doen opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan; 2° de oorsprong of de bestemming van telecommunicatie laten lokaliseren.	§ 1. **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:** **1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;** **2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren**	
In de gevallen bepaald in het eerste lid wordt voor ieder telecommunicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de telecommunicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.	In de gevallen bepaald in het eerste lid wordt voor ieder **elektronisch communicatiemiddel** waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de **elektronische communicatie** wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.	
De onderzoeksrechter vermeldt de feitelijke omstandigheden van de zaak	**De onderzoeksrechter doet in een gemotiveerd bevelschrift opgave van de**	

die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings.	**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.**	
Hij vermeldt ook de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing.	**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.**	
In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter. Indien het echter het in artikel 347bis of 470 van het Strafwetboek bedoelde strafbare feit betreft, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.	In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter. Indien het echter het in artikel 347bis of 470 van het Strafwetboek bedoelde strafbare feit betreft, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.	
De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.	De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.	
	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	
	§ 2. Wat betreft de toepassing van de maatregel bedoeld in § 1 op de verkeers- of lokalisatiegegevens die	

	worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing: - **Voor een strafbaar feit bedoeld in Titel Iter van Boek II van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift.** - **Voor andere strafbare feiten 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 vijf jaar of een zwaardere straf tot gevolg kunnen hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;** - **Voor andere strafbare feiten niet bedoeld in de vorige twee onderdelen, 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.** **§ 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 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.	
§2. Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst deelt de gegevens waarom verzocht werd mee binnen een termijn te bepalen door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig frank tot tienduizend frank (lees euro).	**§4. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst** deelt de gegevens waarom verzocht werd mee binnen een termijn te bepalen door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. Iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig frank tot tienduizend frank (lees euro).	
Artikel 90decies De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.	**Article 90decies** De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.	Artikel 10 wetsontwerp

Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter. Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven. Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.	Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter. Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten. Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven. Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. **<u>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.</u>**	
	HOOFDSTUK 4. –Wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten	
Artikel 13. In het raam van hun opdrachten kunnen de inlichtingen- en	**Artikel 13.** In het raam van hun opdrachten kunnen de inlichtingen- en	Artikel 11 wetsontwerp

veiligheidsdiensten inlichtingen en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten. De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien. De inlichtingen- en veiligheidsdiensten die gebruik maken van de methoden voor het verzamelen van gegevens als bedoeld in de onderafdelingen 2 en 2bis dienen te waken over de veiligheid van de gegevens die betrekking hebben op menselijke bronnen en over de informatie die zij meedelen.	veiligheidsdiensten ~~**inlichtingen**~~ **informatie** en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten. De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien. ~~**De inlichtingen- en veiligheidsdiensten die gebruik maken van de methoden voor het verzamelen van gegevens als bedoeld in de onderafdelingen 2 en 2bis dienen te waken over de veiligheid van de gegevens die betrekking hebben op menselijke bronnen en over de informatie die zij meedelen.**~~ **De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die zij leveren.** **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.**	
Artikel 18/3. §1. Rekening houdend met een potentiële bedreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die	**Article 18/3.** §1. Rekening houdend met een potentiële bedreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die	Artikel 12 wetsontwerp

nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële bedreiging waarvoor ze wordt aangewend. De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie. De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen-en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd. De inlichtingenofficier die is aangesteld om de specifieke methode voor het verzamelen van gegevens aan te wenden, informeert het diensthoofd regelmatig over de uitvoering van deze methode. §2. Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie. De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.	nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële bedreiging waarvoor ze wordt aangewend. De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie. ~~**De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen-en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd.**~~ ~~**De inlichtingenofficier die is aangesteld om de specifieke methode voor het verzamelen van gegevens aan te wenden, informeert het diensthoofd regelmatig over de uitvoering van deze methode.**~~ **§2.** ~~**Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.**~~ ~~**De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.**~~	

Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen- en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	~~Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe eigenen en de leden van de dienst horen.~~	
De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen-en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.	~~De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.~~	
De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.	~~De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.~~ **De beslissing van het diensthoofd vermeldt:** **1° de aard van de specifieke methode;** **2° naargelang het geval, de natuurlijke perso(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 dreiging 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 Commissie;** **6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen ;**	

	7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode; **8° in voorkomend geval, de samenloop met een 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 dreiging;** **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.**	
§3. De lijsten bedoeld in § 2 bevatten de volgende gegevens : 1° de aard van de specifieke methode voor het verzamelen van gegevens; 2° de graad van de ernst van de bedreiging die de specifieke methode voor het verzamelen van gegevens wettigt; 3° naargelang het geval, de natuurlijke of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode voor het verzamelen van gegevens; 4° het technische middel dat gebruikt wordt om de specifieke methode voor het verzamelen van gegevens aan te wenden; 5° de periode tijdens welke de specifieke methode voor het verzamelen van gegevens kan worden uitgevoerd te rekenen van de beslissing.	**§3.** ~~**De lijsten bedoeld in § 2 bevatten de volgende gegevens :**~~ ~~**1° de aard van de specifieke methode voor het verzamelen van gegevens;**~~ ~~**2° de graad van de ernst van de bedreiging die de specifieke methode voor het verzamelen van gegevens wettigt;**~~ ~~**3° naargelang het geval, de natuurlijke of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode voor het verzamelen van gegevens;**~~ ~~**4° het technische middel dat gebruikt wordt om de specifieke methode voor het verzamelen van gegevens aan te wenden;**~~ ~~**5° de periode tijdens welke de specifieke methode voor het verzamelen van gegevens kan worden uitgevoerd te rekenen van de beslissing.**~~ **Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.**	

	Deze lijsten bevatten de gegevens bedoeld in §2, 1° tot 3°, 5° en 7°.	
§4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.	§4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.	
	§5. De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen-en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd.	
	§6. De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit.	
	Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen-en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	
	De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de comissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de	

	commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen-en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is. **De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.** **§7. De inlichtingenofficier die is aangesteld ~~om de specifieke methode voor het verzamelen van gegevens aan te wenden~~ om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen, informeert het diensthoofd regelmatig over de uitvoering van deze methode.** **§8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging 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.**	
Artikel 18/8. §1. Wanneer dit een belang vertoont voor de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, zo nodig door daartoe de technische medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot : 1° het opsporen van de oproepgegevens van elektronische communicatiemiddelen van waaruit of waarnaar oproepen worden of werden gericht;	**Article 18/8. §1. ~~Wanneer dit een belang vertoont voor de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, zo nodig door daartoe de technische medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot :~~** **~~1° het opsporen van de oproepgegevens van elektronische communicatiemiddelen van waaruit of waarnaar oproepen worden of werden gericht;~~**	Artikel 13 wetsontwerp

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.	~~**2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.**~~ **De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:** **1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;** **2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.**	
In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.	In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de ~~**oproepgegevens**~~ **verkeersgegevens** worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.	
De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	
§2. In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze	**§2.** ~~**In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze**~~	

mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd. De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	~~**mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd.**~~ ~~**De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.**~~ **Wat betreft de toepassing van de methode bedoeld in § 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:** **1°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing.** **2°) Voor een potentiële dreiging zoals bedoeld in artikel 18/1, andere dan deze bedoeld in 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing.** **3°) Voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing.**	
§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de	§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de	

gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie. Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.	gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie. Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro. **§4. In geval van uiterst dringende met redenen omklede noodzakelijkheid kan de inlichtingenofficier deze gegevens bij mondelinge beslissing ogenblikkelijk vorderen mits voorafgaand mondeling akkoord van het diensthoofd. Deze mondelinge beslissing wordt zo spoedig mogelijk bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd.** **De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.**	

Projet de loi relative à
la conservation des données dans le secteur des communications électroniques

TEXTE DE BASE	TEXTE DE BASE ADAPTE AU PROJET	Article du projet de loi
	CHAPITRE 2. – Modifications de la loi du 13 juin 2005 relative aux communications électroniques	
Article 2. Pour l'application de la présente loi, il faut entendre par : […] 11° " opérateur " : toute personne ayant introduit une notification conformément à l'article 9; […]	**Article 2.** Les modifications suivantes sont apportées : […] ***11° "opérateur" : toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;*** […] ***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.***	Article 2 du projet
Article 125. § 2. Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en oeuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques.	[…]	Article 3 du projet
Article 126. § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en	***Article 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 opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, 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.*** ***Le présent article ne porte pas sur le contenu des communications.***	Article 4 du projet

vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. § 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut. Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique.	***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° 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° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.*** ***§ 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° 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° Les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil 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.*** ***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. ***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 et 2, 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 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.*** ***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. ***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. 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 et 3, 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.*** ***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, sont conservées pendant douze 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, sont conservées pendant douze 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 3 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 ;*** ***4° conservent les données sur le territoire de l'Union européenne ;*** ***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° 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° 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. L'Institut et la Commission pour la protection de la vie privée concluent un***	

	protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal. ***§ 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.*** ***Ces statistiques comprennent notamment :*** ***1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;*** ***2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;*** ***3° les cas dans lesquels des demandes de données 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 90decies 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.	
	Article 126/1. § 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 l'appelant en vertu de l'article 107, § 2, alinéa 1er ou les données qui peuvent être requises en vertu des articles 46bis, 88bis et 90ter 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. ***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.*** ***Afin de faire partie de la Cellule coordination, il faut au préalable répondre aux conditions cumulatives suivantes :*** ***1° Avoir fait l'objet d'un avis de sécurité positif et non périmé conformément à l'article 22quinquies 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.***	Article 5 du projet

	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. ***Les opérateurs et fournisseurs qui ne fournissent aucun des services visés à l'article 126, § 1er, sont dispensés de la condition visée à l'alinéa 3, 1°.*** ***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.*** ***Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.*** ***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 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. 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.*** ***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. ***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. 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.*** ***Plusieurs opérateurs ou fournisseurs peuvent désigner un ou plusieurs préposés à la protection des données à caractère personnel communs. En pareil cas, ce ou ces préposé(s) doi(ven)t assurer la même mission pour chaque opérateur ou fournisseur individuel.*** ***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.*** ***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. ***Le préposé doit avoir la possibilité de communiquer directement avec la direction de l'opérateur ou du fournisseur.*** ***Le préposé à la protection des données veille à ce que :*** ***1° les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi ;*** ***2° le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver ;*** ***3° seules les autorités légalement autorisées aient accès aux données conservées ;*** ***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.*** ***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. 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° les modalités de la demande et de l'octroi de l'avis de sécurité ;*** ***2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en***	

	compte ***la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger ;*** ***3° 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 ;*** ***4° 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, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande ».***	
Article 127. § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre : 1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence; 2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les	**Article 127.** § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, ***aux fournisseurs visés à l'article 126, § 1er, alinéa 1er,*** ou aux utilisateurs finals, en vue de permettre : 1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence; 2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs ***et des fournisseurs visés à l'article 126, § 1er, alinéa 1er***, aux	Article 6 du projet

opérateurs ou les abonnés doivent donner suite aux mesures imposées.	opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.	
§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	
§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.	§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.	
§ 4. Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.	§ 4. Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.	
§ 5. Les opérateurs déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion. Si un opérateur ne déconnecte pas les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible.	§ 5. Les opérateurs déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion. Si un opérateur ne déconnecte pas les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible.	
§ 6. Chaque opérateur établit, sur la base du paragraphe 1er, une procédure interne permettant de répondre aux demandes	[…]	

d'accès 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.		
Article 145. § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 114, 124, 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47 et 127. § 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16. § 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement : 1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite; 2° (abroge) 3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci. § 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de	**Article 145.** § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 114, 124, ***126, 126/1,*** 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, ***126, 126/1*** et 127. § 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16. § 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement : 1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite; 2° (abroge) 3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci. § 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de	Article 7 du projet

provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.	provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.	
	§ 3ter. Est puni d'une amende de 50 euros à 50.000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :	
	1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126 ;	
	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.	
§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.	§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.	
	CHAPITRE 3. – Dispositions modifiant le Code d'instruction criminelle	
Article 46bis	**Article 46bis**	Article 8 du projet
§ 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, en requérant au besoin le concours de l'opérateur d'une réseau de communication électronique ou d'un fournisseur d'un service de communication électronique ou d'un service de police désigné par le Roi, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au	§ 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, en requérant au besoin le concours de l'opérateur d'une réseau de communication électronique ou d'un fournisseur d'un service de communication électronique ou d'un service de police désigné par le Roi, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au	

moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur de service à : 1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilise; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence. §2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications.	moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur de service à : 1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilise; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence. **Pour des infractions qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées au premier alinéa que pour une période de six mois préalable à sa décision.** §2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications.	

Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Le refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros.	Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Le refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros.	
Article 88bis 1er. Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication : 1° au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés; 2° a la localisation de l'origine ou de la destination de télécommunications.	**Article 88bis** 1er. **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° 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.**	Article 9 du projet

Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisé, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal.	Dans les cas visés à l'alinéa 1er, pour **moyen de communication électronique** dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisé, le jour, l'heure, la durée et, si nécessaire, le lieu de **la communication électronique** sont indiqués et consignés dans un procès-verbal.	
Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi.	**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.**	
Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement.	**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.**	
En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction. S'il s'agit toutefois de l'infraction visée à l'article 347bis ou 470 du Code pénal, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction soit nécessaire.	En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction. S'il s'agit toutefois de l'infraction visée à l'article 347bis ou 470 du Code pénal, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction soit nécessaire.	
Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.	Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.	

	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. **§ 2. Pour ce qui concerne l'application de la mesure visée au § 1er aux données de trafic ou de localisation conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent:** - **Pour une infraction visée au Titre Iter du Livre II du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance.** - **Pour les autres infractions 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 pour une période de neuf mois préalable à l'ordonnance.** - **Pour d'autres infractions non visées par les deux points précédents, 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.** **§ 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 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.**	
§ 2. Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication communique les informations qui ont été demandées dans un délai a fixer par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.	**§4. 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** communique les informations qui ont été demandées dans un délai a fixer par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.	
Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les Télécommunications, est punie d'une amende de vingt-six francs (lire euros) à dix mille francs (lire euros).	Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les Télécommunications, est punie d'une amende de vingt-six francs (lire euros) à dix mille francs (lire euros).	
Article 90decies Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.	**Article 90decies** Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.	Article 10 du projet

Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus. Il fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter. Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés.	Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus. Il fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter. Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés. **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	
Article 13. Dans le cadre de leurs missions, ils peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.	**Article 13.** Dans le cadre de leurs missions, ils peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.	Article 11 du projet

Les services de renseignement et de sécurité qui ont recours aux méthodes de recueil de données visées aux sous-sections 2 et 2bis doivent veiller à la sécurité des données ayant trait aux sources humaines et aux informations qu'elles communiquent.	~~**Les services de renseignement et de sécurité qui ont recours aux méthodes de recueil de données visées aux sous-sections 2 et 2bis doivent veiller à la sécurité des données ayant trait aux sources humaines et aux informations qu'elles communiquent.**~~ **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.** **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.**	
Article 18/3. §1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en oeuvre compte tenu de la menace potentielle visée à l'article 18/1, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en oeuvre. La méthode spécifique ne peut être mise en oeuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission. Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices	**Article 18/3.** §1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en oeuvre compte tenu de la menace potentielle visée à l'article 18/1, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en oeuvre. La méthode spécifique ne peut être mise en oeuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission. ~~**Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable**~~	Article 12 du projet

sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.	~~d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.~~	
L'officier de renseignement désigné pour mettre en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.	~~L'officier de renseignement désigné pour mettre en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.~~	
§2. Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.	**§2.** ~~Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.~~	
Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.	~~Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.~~	
Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.	~~Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.~~	
Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.	~~Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.~~	
La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.	~~La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.~~	

	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 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.**	
§3. Les listes visées au § 2 comprennent les données suivantes : 1° la nature de la méthode spécifique de recueil de données; 2° le degré de gravité de la menace qui justifie la méthode spécifique de recueil de données; 3° selon le cas, la ou les personnes	**§3. ~~Les listes visées au § 2 comprennent les données suivantes :~~** **~~1° la nature de la méthode spécifique de recueil de données;~~** **~~2° le degré de gravité de la menace qui justifie la méthode spécifique de recueil de données;~~** **~~3° 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 de recueil de données; 4° le moyen technique employé pour mettre en oeuvre la méthode spécifique de recueil des données; 5° la période durant laquelle la méthode spécifique de recueil de données peut être mise en oeuvre à compter de la décision.	~~**physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique de recueil de données;**~~ ~~**4° le moyen technique employé pour mettre en oeuvre la méthode spécifique de recueil des données;**~~ ~~**5° la période durant laquelle la méthode spécifique de recueil de données peut être mise en oeuvre à compter de la décision.**~~ **Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.** **Ces listes comprennent les données visées au §2, 1° à 3°, 5° et 7°.**	
§4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er.	§4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er. **§5. Les méthodes spécifiques ne peuvent être mise en oeuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.** **§6. Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.** **Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées**	

	les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service. **Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en oeuvre si celle-ci est toujours en cours.** **La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.** **§7. L'officier de renseignement désigné pour ~~mettre~~ le suivi de la mise en oeuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.** **§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 oeuvre, ou quand il a été constaté une illégalité. Il informe dès que possible la commission de sa décision.**	
Article 18/8. §1er. Lorsque cela présente un intérêt pour l'exercice des missions, le dirigeant du service peut, par une décision écrite, procéder ou faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques :	**Article 18/8. §1er. ~~Lorsque cela présente un intérêt pour l'exercice des missions, le dirigeant du service peut, par une décision écrite, procéder ou faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques :~~**	Article 13 du projet

1° au repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés; 2° à la localisation de l'origine ou de la destination de communications électroniques.	~~**1° au repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;**~~ ~~**2° à la localisation de l'origine ou de la destination de communications électroniques.**~~ **Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de 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 adressées ou ont été adressées ;** **2° à la localisation de l'origine ou de la destination de communications électroniques.**	
Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les données d'appel sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.	Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les ~~**données d'appel**~~ **données de trafic** sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.	
La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	
§2. En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et préalable	~~***§2.* En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et***~~	

du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service. La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	~~**préalable du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service.**~~ ~~**La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.**~~ **Pour ce qui concerne l'application de la méthode visée au § 1er aux données conservées sur base de l'article 126 de la Loi sur les communications électroniques, les dispositions suivantes s'appliquent :** **1°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut requérir les données que pour une période de six mois préalable à la décision.** **2°) Pour une menace potentielle autre que celles visées sous 1° et 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision.** **3°) Pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision.**	
§3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les	*§3.* Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les	

Communications électroniques dans ses attributions. Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à dix mille euros.	Communications électroniques dans ses attributions. Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à dix mille euros. **§4. En cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir ces données sur-le-champ, avec l'accord verbal et préalable du dirigeant du service. Cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service.** **La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.**	